LANDesk®

Management Suite 9.5

Guia do usuário

LANDesk® SOFTWARE

Copyright © 2002-2012, LANDesk Software, Inc. e suas afiliadas. Todos os direitos reservados. A LANDesk e seus logotipos são marcas registradas ou marcas comerciais da LANDesk Software, Inc. e suas afiliadas nos Estados Unidos e/ou outros países. Outras marcas e nomes podem ser reivindicados como propriedade de outras empresas.

A LANDesk não garante que este documento é livre de erros e retém o direito de fazer mudanças neste documento ou especificações de produtos relacionados e descrições a qualquer momento sem aviso prévio. A LANDesk não assume qualquer obrigação de atualizar as informações aqui contidas. Este documento é fornecido "NO ESTADO EM QUE SE ENCONTRA" sem garantias ou licenças de qualquer tipo sejam elas expressas ou implícitas, incluindo, mas não limitadas a: adequação a um propósito específico, comerciabilidade, não violação de propriedade intelectual ou outros direitos de terceiros. Os produtos da LANDesk citados neste documento não são destinados ao uso em aplicações médicas, de salvamento ou sustentação à vida. Terceiros podem possuir direitos de propriedade intelectual relevantes a este documento e às tecnologias nele discutidas.

Última revisão em: 12/20/2012

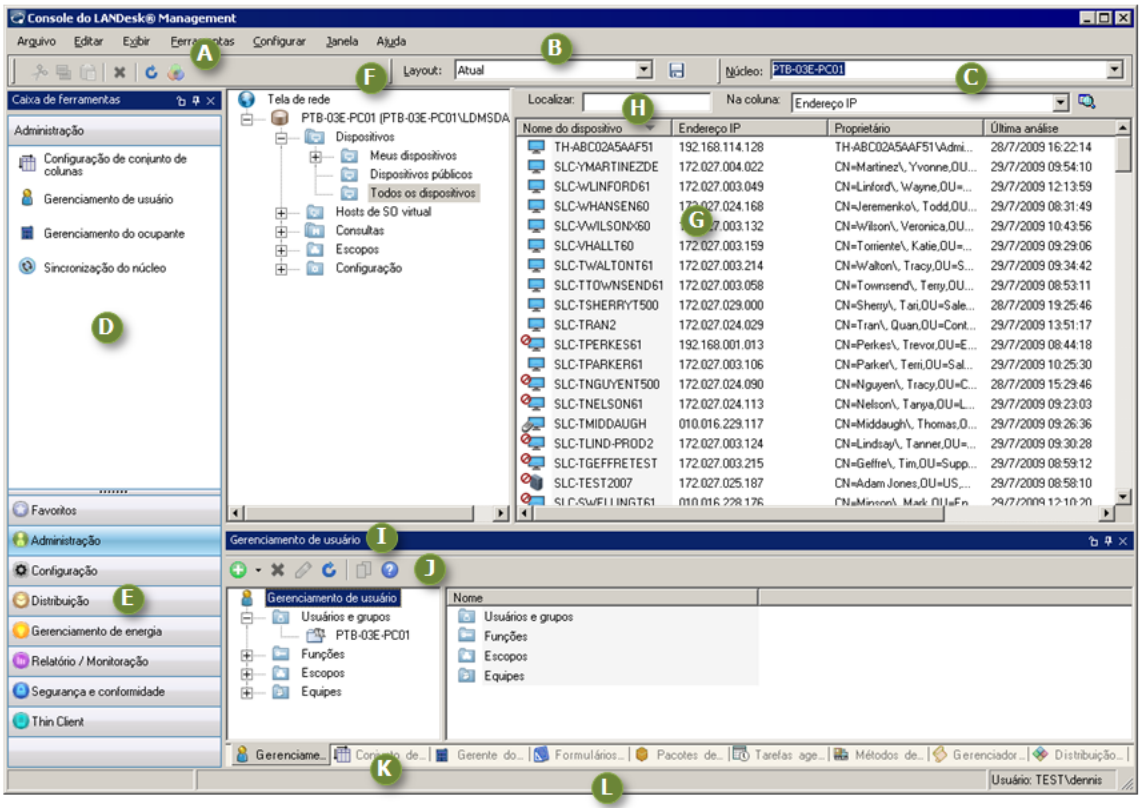
Conteúdo

Conteúdo 3
Console 4
Gerenciamento de usuários 38
Configuração do núcleo 59
Configuração do serviço de núcleo 80
Sincronização do núcleo 92
Configuração de agentes 99
Monitorador de agentes (Agente Watcher) 140
Inventário 147
Gerenciador de diretórios/consultas 183
Auditoria 190
Relatórios 197
Agendamento de tarefas 227
Agendador local 240
Controle remoto 247
Distribuição de softwares/Distribuição de pacotes/Métodos de entrega 258
Application policy management (APM) 305
Monitoramento de licenças de software 310
Descoberta de dispositivos não gerenciados 346
Distribuição do SO 362
Provisionamento 423
LANDesk SmartVue 463
Contas locais 474
Gerenciamento de dispositivos Macintosh 480
Introdução ao LANDesk Security Suite 500
Controle de acesso à rede (NAC) 511
Patch e conformidade 549
Configurações de segurança 656
Atividade da segurança 668
Segurança de ponto final 675
LANDesk Antivirus 712
Proteção de dados da Credant 761
Gerenciador de link do LaunchPad 771
Gerenciamento de energia 774
Alertas 790
Intel vPro 833
Núcleos de rollup 859
Servidores preferenciais e replicação de conteúdo 866
Gerenciamento de ocupantes 879
Virtualização de aplicativos 884
Web console 887
Gerenciador de inventário 940
Gerenciamento de hardwares HP 941

Console

Visão geral do console

O console do Administrador da LANDesk permite você execute todas funções de gerenciamento de rede a partir de um único local. Com um único console, você pode distribuir e atualizar o software ou as configurações, diagnosticar problemas de hardware e software, distribuir imagens do SO e migrar perfis de usuários, utilizar a administração com base em funções para controlar o acesso de usuário a recursos e dispositivos, utilizar recursos de controle remoto para treinar usuários finais ou solucionar problemas e muito mais.



***A** Barra Ferramentas do console, **B** Menu do layout, **C** Menu do Servidor núcleo, **D** Ferramentas, **E** Grupos de ferramentas, **F** Tela de rede, **G** Lista de resultados, **H** Barra Localizar, **I** Painel de ferramentas, **J** Barra de ferramentas Ferramentas, **K** Guias de ferramentas, **L** Barra de status*

Os tópicos de ajuda nesta seção explica como navegar e usar o console a fim de exibir e organizar dispositivos e de como acessar diversas ferramentas de gerenciamento.

Obtendo informações completas e atualizadas sobre instalações e configurações

Você pode ter vários servidores núcleo e bancos de dados para atender às suas necessidades específicas de gerenciamento de rede. Para obter informações sobre a instalação de um servidor núcleo e de um console, consoles adicionais, console Web e gerenciamento de múltiplos servidores núcleo e bancos de dados, consulte a documentação existente na Comunidade de usuários da LANDesk.

NOTA: A Comunidade de usuários da LANDesk
A Comunidade de usuários LANDesk tem fóruns de usuários e os melhores métodos conhecidos para todos os produtos e tecnologia da LANDesk. Para acessar esse recurso valioso, visite: Página inicial da Comunidade de usuários da LANDesk

Tópicos relacionados

Assistentes de configuração do console

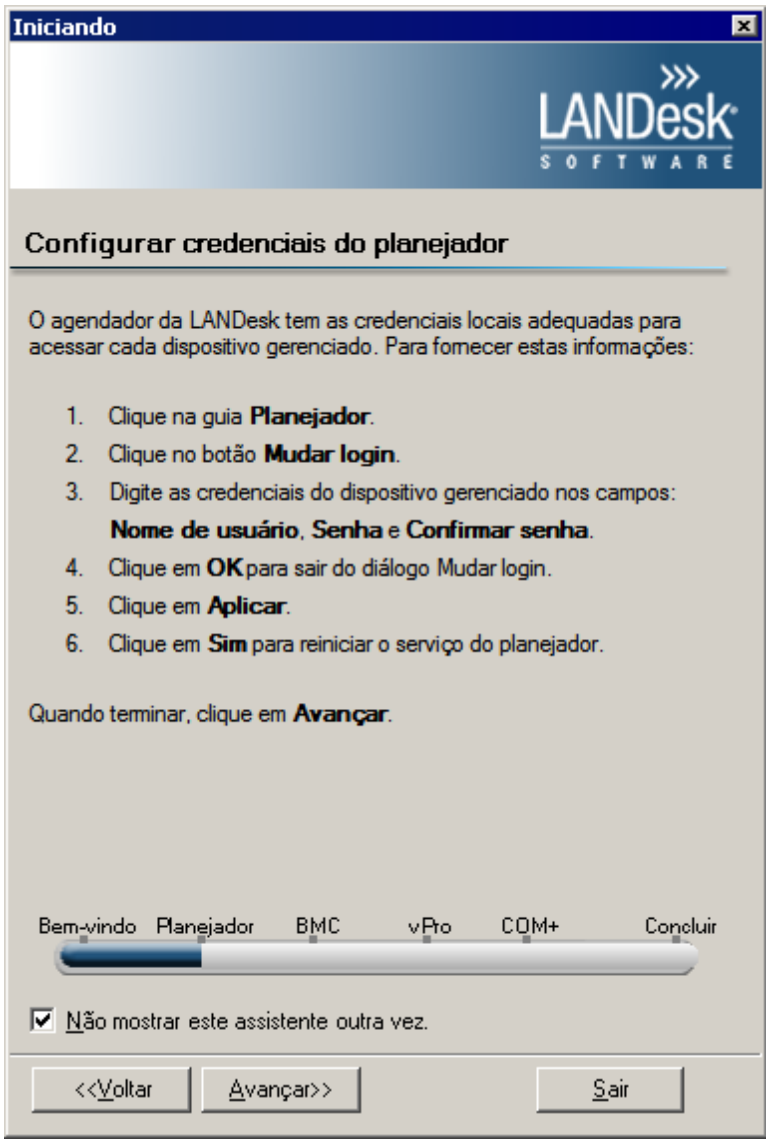
Os assistentes estão disponíveis para várias áreas do LANDesk Management Suite. Estes assistentes continuam por uma série de instruções a medida que o usuário completa os passos descritos.

Os assistentes são exibidos automaticamente em uma nova instalação e podem ser acessados a qualquer momento a partir do menu **Help**. Você pode seguir os passos do assistente para aprender mais sobre o recurso específico ou funcionalidade. Ou você pode marcar a caixa de seleção **Não exibir mais este assistente** para prevenir que o assistente seja exibido automaticamente.

Assistente de início

O assistente de **Introdução** ajuda você a configurar o LANDesk Management Suite para executar as funções a seguir:

- Agendar as tarefas nos dispositivos gerenciados
- Gerenciar dispositivos Intel® vPro e IPMI
- Controlar remotamente dispositivos gerenciados
- Ver usuários de domínio no Console Web


Iniciando
LANDesk
SOFTWARE
Configurar credenciais do planejador
O agendador da LANDesk tem as credenciais locais adequadas para acessar cada dispositivo gerenciado. Para fornecer estas informações:
1. Clique na guia Planejador.
2. Clique no botão Mudar login.
3. Digite as credenciais do dispositivo gerenciado nos campos: Nome de usuário, Senha e Confirmar senha.
4. Clique em OK para sair do diálogo Mudar login.
5. Clique em Aplicar.
6. Clique em Sim para reiniciar o serviço do planejador.
Quando terminar, clique em Avançar.
Bem-vindo
Planejador
BMC
vPro
COM+
Concluir
Não mostrar este assistente outra vez.
<<Voltar
Avançar>>
Sair

Assistente dos agentes de descoberta e instalação

O assistente dos **Agentes de descoberta e instalação** ajudam o usuário a configurar o LANDesk Management Suite para executar as seguintes funções:

- Descoberta: Procurar dispositivos na rede que são desconhecidos ao LANDesk Management Suite. Podem ser especificados intervalos de endereços IP para análise na rede.
- Distribuição de um agente: Instala o agente LANDesk Management nos dispositivos a serem gerenciados.

Assistente de Atualizações seguras

O assistente de **Download atualizações de patch** ajuda o usuário a descarregar e gerenciar arquivos de definições de vulnerabilidade de segurança e patch dos servidores de conteúdo LANDesk. O assistente ajuda na configuração de tarefas para descarregar atualizações, iniciar a tarefa e agendar futuros downloads.

Assistente de criação de funções e grupos

O assistente de **Gerenciamento de usuários** ajuda na execução das etapas necessárias para gerenciar quem pode acessar dispositivos na rede e que ferramentas ou recursos específicos podem ser usados nesses dispositivos. Ele o guia através do processo de criar um escopo, uma função e uma permissão de grupo de usuário.

Iniciar o console

Para iniciar o console

1. Clique em **Iniciar** > **Programas** > LANDesk > Management Suite. (O nome real do programa pode ser diferente, dependendo do produto LANDesk instalado e da licença usada para ativar o servidor núcleo.)
2. Digite o nome de usuário e a senha.

   Se você estiver se conectando a um servidor núcleo remoto, siga as regras normais do Windows para login remoto (ou seja, se o usuário estiver no mesmo servidor núcleo, basta informar o nome do usuário; se o usuário for um usuário do domínio, digite o nome do domínio\nome de usuário).
3. Selecione o servidor núcleo ao qual deseja se conectar. O usuário deve ter credenciais de autenticação adequadas para esse servidor núcleo.
4. Clique em **OK**.

O console é aberto com o layout (tamanho, posição, janelas de ferramentas abertas, etc.) usado na última vez em que o usuário fez logout.

Para os consoles adicionais, as credenciais usadas para acessar o Management Suite devem corresponder às credenciais usadas para qualquer unidade que tiver mapeado para o servidor núcleo. Caso contrário, pode aparecer o erro "Múltiplas conexões" na caixa de diálogo de login do console.

Sobre a caixa de diálogo Login

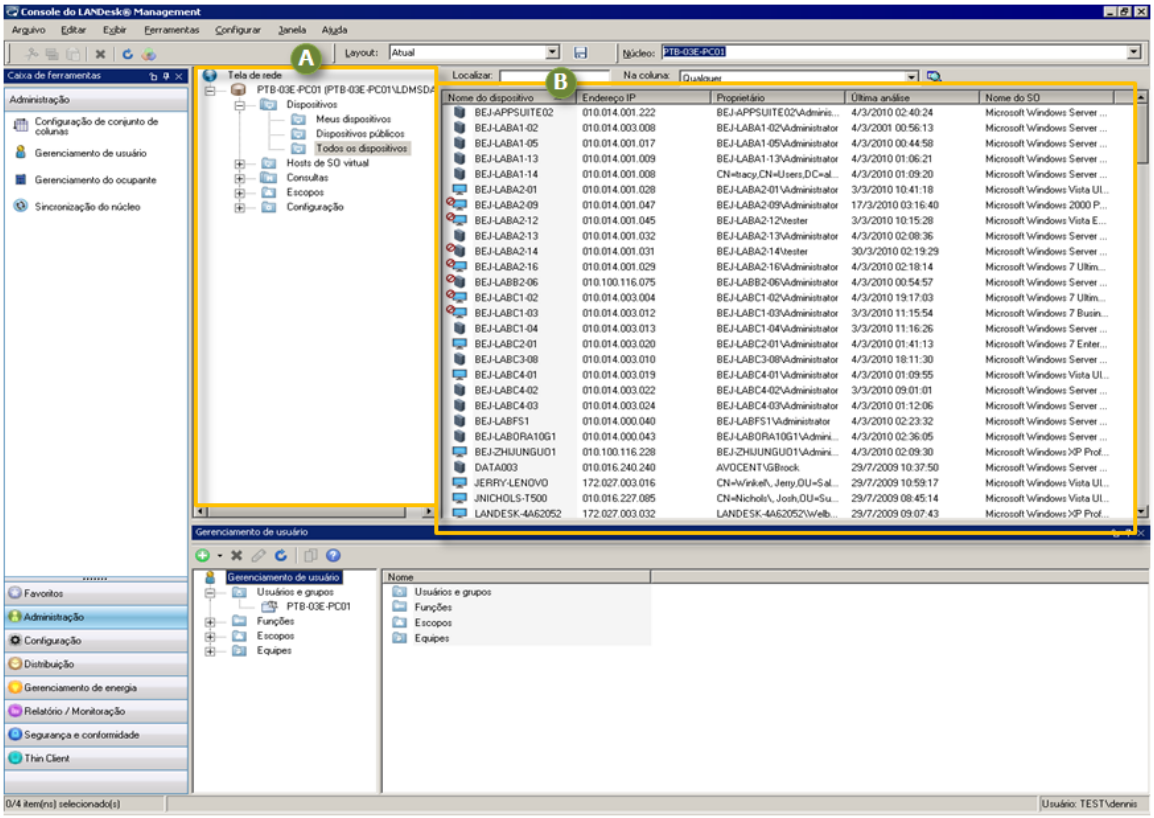
Use esse diálogo para iniciar o console e conectar-se a um servidor núcleo.

- **Nome de usuário:** Identifica um usuário LANDesk. Esse usuário pode ser um administrador ou outro tipo de usuário com acesso restrito (consulte "Gerenciamento de usuários" na página 38). O usuário deve ser um membro dos grupos LANDesk no servidor núcleo. Siga as regras normais do Windows para login remoto (ou seja, se o usuário estiver no mesmo servidor núcleo, basta digitar o nome do usuário; se o usuário for um usuário do domínio, digite o nome do domínio\nome de usuário).
- **Senha:** a senha do usuário. (**NOTA:** Se um administrador do LANDesk mudar a senha de outro usuário, por exemplo um usuário do console adicional, a nova senha não entrará em vigor até que esse usuário reinicialize seu console. Nesse momento, o usuário deverá digitar sua nova senha para fazer login no console.)
- **Servidor núcleo:** especifica o servidor núcleo ao qual você deseja se conectar. Essa lista suspensa é a mesma lista suspensa de servidores núcleo disponível na barra de ferramentas do console.

Entenda a Tela de rede

A Tela de rede é a janela principal do console e o ponto de partida para a maioria das tarefas administrativas. É na Tela de rede que você vê os dados de inventário do dispositivo, cria consultas para procurar e agrupar dispositivos, seleciona dispositivos para controlar remotamente e assim por diante.

A janela da Tela de rede está sempre aberta e contém dois painéis. O painel esquerdo **(A)** mostra uma árvore hierárquica do banco de servidor núcleo/banco de dados ao qual você está atualmente conectado aos grupos **Dispositivos**, **Consultas** e **Configuração**. É possível expandir ou recolher os objetos da árvore, conforme a necessidade. O painel direito **(B)** na Tela da rede exibe uma lista detalhada de itens do grupo selecionado.



***A** Painel da tela de rede, **B** Exibição de itens selecionados na lista*

A janela da Tela de rede, assim como seus painéis e suas colunas podem ser redimensionados, mas não fechados. A janela da Tela de rede não pode ser encaixada como as janelas de ferramentas.

NOTA: Administração com base em funções
Os dispositivos que podem ser visualizados e gerenciados na Tela de rede, além das ferramentas de gerenciamento que podem ser usadas, são determinados pelos direitos de acesso e pelo escopo de dispositivos atribuídos a você pelo administrador. Para obter mais informações, consulte "Gerenciamento de usuários" na página 38.

A **Tela de rede** contém os seguintes grupos e subgrupos:

Núcleo

O objeto **Núcleo** identifica o servidor núcleo ao qual você está conectado no momento. O objeto **Núcleo** está localizado diretamente sob a raiz da Tela de rede, podendo ser ampliado e reduzido.

Sintaxe de nome do objeto núcleo

A sintaxe do nome do objeto núcleo é a seguinte:

Nome do servidor\Instância do banco de dados

Dispositivos

O grupo **Dispositivos** contém os seguintes subgrupos de dispositivos.

- **Meus dispositivos:** Relaciona os dispositivos do usuário atualmente conectado, de acordo com o escopo desse usuário. O usuário pode criar subgrupos de dispositivos apenas em **Meus dispositivos**. Os usuários podem adicionar dispositivos no seu grupo **Meus dispositivos** ou em qualquer um dos seus subgrupos, por meio de cópia dos grupos **Dispositivos públicos** e **Todos os dispositivos**. Os usuários também podem clicar e arrastar dispositivos de **Dispositivos públicos** e **Todos os dispositivos** para o grupo **Meus dispositivos**.

NOTA: Arrastar e soltar itens na Tela de rede
Quando você clica em um item para arrastá-lo para outro grupo na Tela de rede, o cursor indica em que local você pode ou não soltar o item. Ao passar o cursor sobre um objeto do grupo, um sinal de mais (+) indica que é possível incluir o item nesse grupo; e um símbolo "vazio" (um círculo com uma barra inclinada no meio) indica que você não pode incluir o item nesse grupo.

- **Dispositivos públicos:** Relaciona os dispositivos que um administrador (um usuário com direito de administrador LANDesk) adicionou a partir do grupo **Todos os dispositivos**. O administrador vê todos os dispositivos neste grupo, mas os outros usuários só podem ver os dispositivos permitidos pelo seus escopos. Além disso, apenas o administrador pode criar um subgrupo em **Dispositivos públicos**.
- **Todos os dispositivos:** Relaciona todos os dispositivos que podem ser vistos pelo usuário atualmente conectado, com base em seu escopo, em uma lista sem subgrupos. Para o administrador, **Todos os dispositivos** relaciona todos os dispositivos gerenciados que foram analisados no banco de dados núcleo. Os dispositivos configurados com o agente LANDesk padrão são exibidos automaticamente no grupo **Todos os dispositivos** quando são analisados e colocados no banco de dados núcleo pelo analisador de inventário.

Para os usuários normais, Todos os dispositivos é uma combinação dos grupos **Meus dispositivos** e **Dispositivos públicos de cada usuário**.

Tanto os administradores quanto os usuários podem emitir relatórios de recursos dos dispositivos deste grupo.

Você também pode adicionar computadores manualmente à tela da rede. Para isso, clique com o botão direito no grupo **Todos os dispositivos**, selecione, clique em **Inserir novo computador**, preencha as informações do dispositivo e da rede e clique em **OK**. Esses computadores também aparecem no subgrupo de Computadores adicionados do usuário no grupo Configuração.

Hosts SO virtuais

O grupo Hosts do SO virtual exibe os servidores do host virtual VMWare ESX. O grupo Hosts SO virtuais contém os seguintes grupos de configuração:

- **Meus hosts SO virtuais:** Relaciona os hosts SO virtuais do usuário atualmente conectado, de acordo com o escopo desse usuário. O usuário pode criar subgrupos de dispositivos apenas em Meus hosts SO virtuais.
  Os usuários podem adicionar dispositivos no seu grupo Meus hosts SO virtuais ou em qualquer um dos seus subgrupos, copiando e colando-os dos grupos de Hosts SO virtuais públicos e Todos os hosts SO virtuais. Os usuários podem também clicar e arrastar hosts SO virtuais dos hosts SO virtuais públicos e Todos os hosts SO virtuais para seus grupos Meus hosts SO virtuais.
- **Hosts SO virtuais públicos:** Relaciona os dispositivos que o administrador Management Suite adicionou do grupo Todos os dispositivos. Os usuários com direito de administrador LANDesk vêm todos os dispositivos neste grupo, mas os outros usuários do do Console só podem ver os dispositivos permitidos pelo seus escopos. Só um administrador pode criar um subgrupo sob Hosts SO virtuais públicos.
- **Todos os hosts SO virtuais:** Relaciona todos os hosts SO virtuais que podem ser vistos pelo usuário atualmente conectado, com base em seu escopo, em uma lista simples (sem subgrupos). Para o administrador, Todos os hosts SO virtuais contém todos os hosts SO virtuais gerenciados que foram analisados para o banco de dados. Os hosts SO virtuais configurados com o Agente LANDesk padrão aparecem automaticamente no grupo/pasta Todos os hosts SO virtual quando são analisados e colocados no banco de dados núcleo pelo analisador de inventário.
- **Hosts do SO virtual do usuário:** Relaciona todos os Hosts do SO virtual no banco de dados (organizado por subgrupos de usuário). Os subgrupos de usuários são nomeados com os IDs de login do usuário (ou seja, nome do computador\conta de usuário ou domínio\conta de usuário). Cada grupo de usuários contém os hosts do SO virtual que são exibidos no grupo Meus Hosts do SO virtual destes usuários.

Consultas

O grupo **Consultas** contém os seguintes subgrupos de consultas.

- **Minhas consultas:** Relaciona as consultas criadas pelo usuário atualmente conectado ou aquelas adicionadas ao grupo de **Consultas de usuário** por um administrador. O usuário pode criar, modificar e excluir grupos de consulta e consultas do seu grupo **Minhas consultas**. Ele também pode copiar consultas do grupo **Consultas públicas** neste grupo.

Toda consulta executada pelo usuário é limitada à gama de dispositivos definida pelo escopo desse usuário. Por exemplo, se o escopo do usuário for **Todas as máquinas**, a consulta pesquisará todos os dispositivos no banco de dados núcleo, mas se o escopo do usuário for restrito a 20 máquinas, apenas essas 20 máquinas serão pesquisadas pela consulta. Para obter mais informações sobre consultas, leia ""Gerenciador de diretórios/consultas" na página 183".

- **Consultas públicas:** Relaciona as consultas que o administrador ou um usuário com direito de PQM (Public Query Management) adicionou. Apenas os usuários com direitos de Administrador LANDesk ou com o direito de PQM podem adicionar, modificar ou excluir grupos de consultas ou consultas no grupo **Consultas públicas**. Entretanto, todos os usuários podem ver as consultas desse grupo e copiá-las para seu próprio grupo **Minhas consultas**.

- **Todas as consultas:** Relaciona todos as consultas que podem ser vistas pelo usuário atualmente conectado, com base em seu escopo, em uma lista sem subgrupos. O grupo **Todas as consultas** é uma combinação dos grupos **Minhas consultas** e **Consultas públicas** do usuário.

Os administradores podem usar esse grupo para executar as consultas de um usuário com base no escopo desse usuário, como se fossem o próprio usuário. Dessa forma, o administrador pode visualizar exatamente os resultados que um usuário obterá ao executar uma consulta.

Escopos

A Tela de rede inclui um atalho para exibir escopos existentes, editar ou criar novos escopos. Você também pode definir os campos que você quer exibir na Tela de rede. Para obter mais detalhes sobre como criar e usar Escopos, consulte "Criar um escopo" na página 55.

Configuração

O grupo **Configuração** contém os seguintes subgrupos de configuração.

- **Fila de retenção PXE:** Relaciona as filas de retenção PXE e os dispositivos que estão nessas filas.
- **Servidor bare metal:** Contém dispositivos bare metal que foram criados para tarefas de provisionamento.
- **Provisionamento de PXE (Windows PE):** Contém dispositivos alvo para tarefas de provisionamento Microsoft Windows PE.
- **Representantes do domínio de multidifusão:** Relaciona os representantes do domínio de multidifusão configurados que podem ser usados para equilíbrio de carga de distribuição de software. Para obter mais informações, consulte "Uso da Multidifusão dirigida com a distribuição de software" na página 272.
- **Representantes PXE:** Relaciona os dispositivos configurados como representantes de PXE que podem distribuir imagens do SO para dispositivos da sua sub-rede.
- **Distribuições pendentes de clientes não gerenciados:** Relaciona dispositivos que foram descobertos pela ferramenta Descoberta de dispositivos não gerenciados e aguardam por uma tarefa de configuração de agentes. Para obter mais informações, consulte "Visão geral da descoberta de dispositivos não gerenciados" na página 346.
- **Computadores adicionados por usuário:** (Somente administradores) Contém computadores que foram adicionados manualmente à Tela de rede através do diálogo Inserir novo computador (clique com botão direito no grupo **Todos os dispositivos**).

Resultados do Inspector

Ao usar o LANDesk Inspector para exibir dados, você pode clicar duas vezes um gráfico na janela do inspetor e exibir os detalhes na janela de resultados do Inspetor.

Ver os resultados que esta maneira faz os dados litigável. Por exemplo, no inspetor Programado de tarefas um mapa pode mostrar quantos dispositivos falhou uma tarefa. Se você clicar duas vezes o mapa, você verá os dispositivos individuais listados na pasta de resultados de Inspetor . Você então pode aplicar uma ação a esses dispositivos (tal como começar de na tarefa) ou vê um relatório com que dados acompanhar.

Os dados na pasta de resultados de Inspetor muda cada vez você clica duas vezes em um mapa em uma janela de inspetor.

Ícones da Tela da rede:

Observe que um um ícone aparece ao lado de cada item na lista de resultados da Tela de rede, para identificar o tipo de dispositivo. Se o agente estiver instalado, o dispositivo ligado, o status da condição etc, uma pequena sobreposição pode aparecer sobre ou ao lado do ícone do dispositivo após você clicar nele.

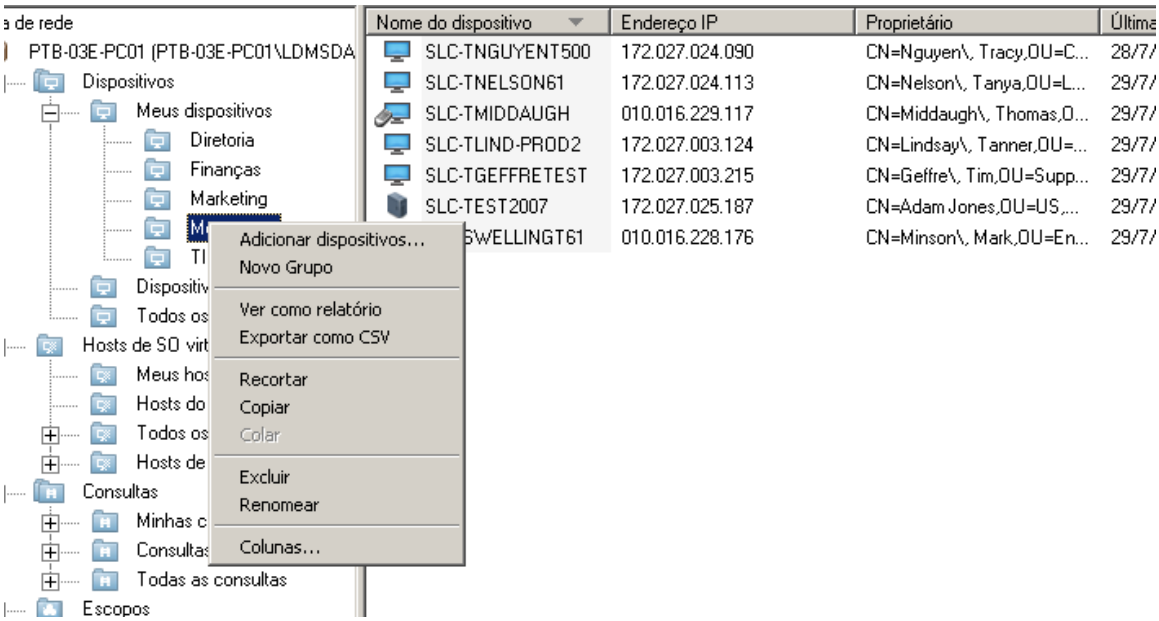
Ícones	Sobreposições
Servidor	LANDesk agent está presente
Desktop	Agente do Controle remoto está presente
Laptop	Status do dispositivo é desconhecido
Dispositivo Móvel	Status do dispositivo indisponível; não conectado
Dispositivo Apple	Dispositivo com alerta de conjunto de regras relatando estado crítico
VMWare host virtual	Dispositivo com alerta de conjunto de regras relatando estado de alerta
VMWare convidado virtual	

Você pode atualizar o agente e o status da condição de dispositivos isoladamente ao selecioná-los na Tela de rede ou de todos os dispositivos visíveis na Tela de rede ao mesmo tempo. Você também pode atualizar o status de um dispositivo, selecionando-o e clicando no botão Atualizar da barra de ferramentas. Para obter mais informações sobre a configuração de como a descoberta de agentes é manipulada, consulte "Configurar descoberta de agentes" na página 99.

NOTA: Qualidade de exibição dos ícones
Esses ícones exigem uma configuração de intensidade de cores de, pelo menos, 16 bits. Se os ícones parecerem fora de foco no seu console, mude suas configurações de cores em Propriedades de exibição do Windows.

Criar grupos na Tela de rede

Os grupos o ajudam a organizar dispositivos e consultas na Tela da rede do console. É possível criar grupos para organizar dispositivos de rede de acordo com a função, a localização geográfica, o departamento, o atributo do dispositivo ou qualquer outra categoria que atenda às suas necessidades. Por exemplo, você pode criar um grupo de marketing para todos os dispositivos do departamento de marketing ou um grupo que inclua todos os dispositivos que utilizam um SO específico.



Regras para a criação de grupos

- **Meus dispositivos e Minhas consultas:** Os administradores e todos os outros usuários podem criar grupos em **Meus dispositivos** e em **Minhas consultas**.
- **Dispositivos públicos:** Apenas os administradores podem criar grupos em **Dispositivos públicos**.
- **Consultas públicas:** Apenas os administradores ou usuários com permissão de "Gerenciamento de consulta pública" podem criar grupos em **Consultas públicas**.
- **Todos os dispositivos e Todas as consultas:** Não existem subgrupos em **Todos os dispositivos** ou **Todas as consultas**. Os usuários, inclusive os administradores, não podem criar grupos em **Todos os dispositivos** ou **Todas as consultas**.

Para criar um grupo

1. Na Tela de rede do console, clique com o botão direito do mouse no grupo-pai (como **Meus dispositivos**) e clique em **Novo grupo**. Ou, selecione o grupo-pai e clique em **Editar** > **Meus dispositivos** > **Novo grupo**.
2. Digite um nome para o novo grupo e, em seguida, pressione a tecla **Enter**.

Agrupar menus de atalho

Você pode clicar com o botão direito do mouse nos grupos para executar várias tarefas, de acordo com o tipo de grupo. Por exemplo, se você criou um subgrupo de dispositivos, o respectivo menu de atalhos fornece diversas opções.

- Adicionar dispositivos
- Novo grupo (Criação de um novo subgrupo)
- Exibir como relatório
- Exportar como CSV
- Recortar
- Copiar

- Colar
- Excluir
- Renomear
- Colunas (selecionar colunas para exibição)

Para obter mais informações sobre os recursos do botão direito, consulte os "Menus de atalho" na página 27

Configurar Tela de rede com conjuntos de colunas

Os conjuntos de colunas permitem personalizar os dados de inventário que aparecem no painel direito da Tela de rede, para as listas de dispositivo e listas de consulta. Cada coluna no conjunto representa um atributo exclusivo (ou componente) do inventário analisado. Por exemplo, o conjunto de colunas padrão que aparece na Tela de rede é composto do atributos Nome do dispositivo, Tipo e Nome do SO.

Use a Ferramenta de configuração de conjunto de coluna (**Ferramentas > Administração > Configuração de conjunto de colunas**) para criar o número de conjuntos de colunas que quiser. Para aplicar um conjunto de colunas, clique e arraste o conjunto de colunas desejado para um grupo de dispositivos ou objetos de consulta na árvore de tela da rede.

Ferramenta de configurações de coluna

A janela ferramenta Conjuntos de colunas organiza os conjuntos em três categorias:

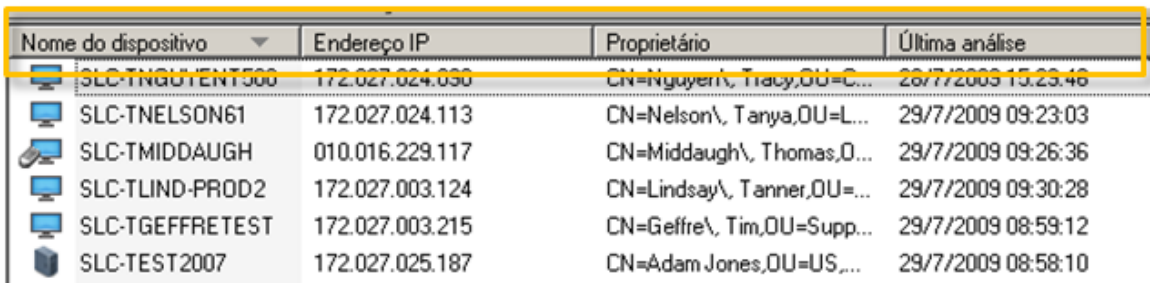
- **Meus conjuntos de colunas:** conjunto de colunas criados pelo usuário conectado atualmente.
- **Conjuntos de colunas públicos:** Conjuntos de coluna criados por um administrador ou conjuntos de colunas predefinidos.
- **Todos os conjuntos de coluna** (visíveis apenas ao administrador): Conjuntos de colunas criados por todos os usuários LANDesk.

Um usuário pode copiar um conjunto de colunas do grupo Conjuntos de colunas públicas para o seu próprio grupo Meus conjuntos de colunas, em seguida, modificar as propriedades do conjunto de colunas.

Você pode criar subgrupos no objeto **Meus conjuntos de colunas** para organizar ainda mais os seus conjuntos de colunas.

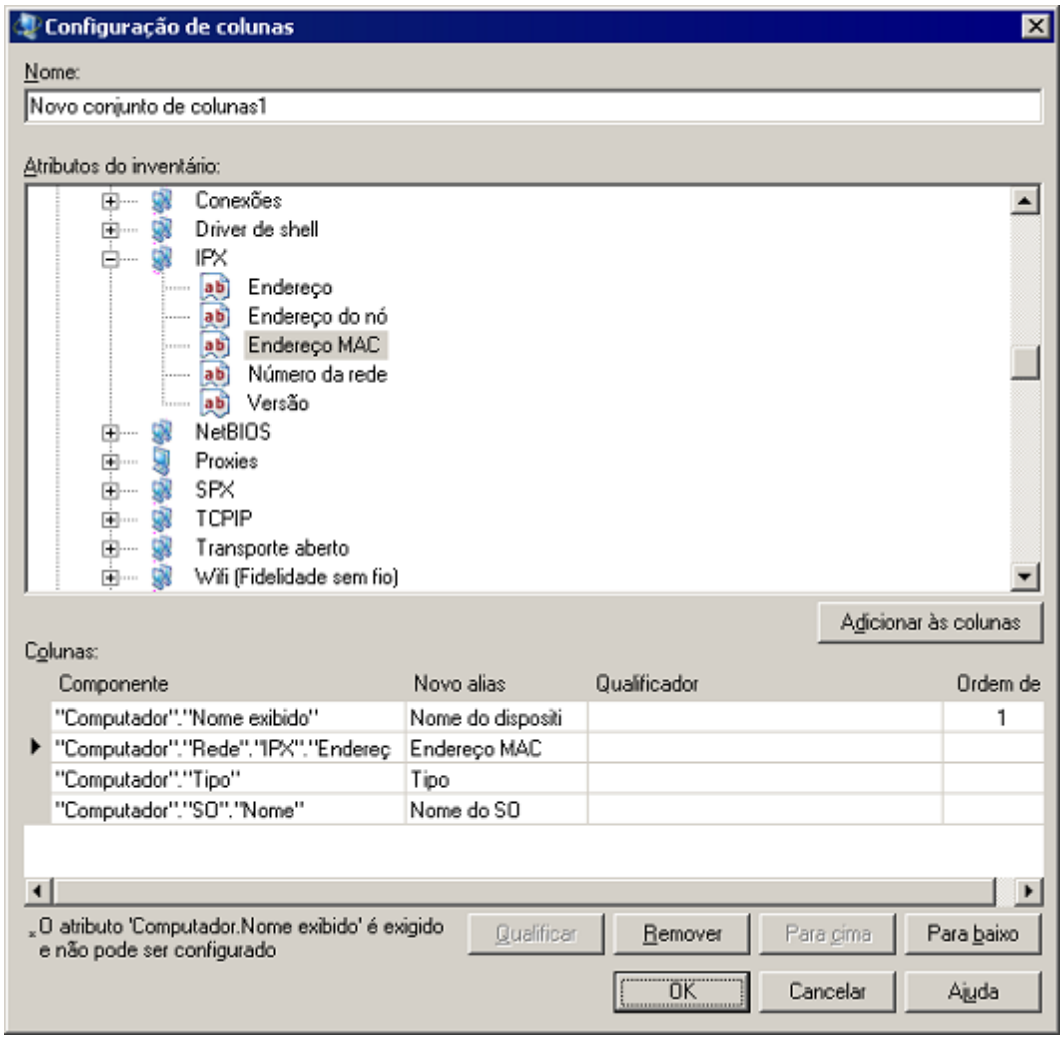
Criar conjuntos de colunas

A caixa de diálogo **Configurações de colunas** é usada para criar os conjuntos de colunas. Cada coluna representa um único atributo de inventário ou o componente que foi analisado no banco de dados núcleo. As colunas são exibidas da direita para a esquerda na Tela de rede. Você pode especificar quais atributos quer incluir ao criar ou editar um conjunto de colunas.



Para criar um conjunto de colunas

1. Clique em **Ferramentas > Administração > Configuração de conjunto de colunas**.
2. Selecione o objeto **Meus conjuntos de colunas** (ou o objeto **Conjuntos de colunas públicas**), em seguida clique no botão **Criar um novo conjunto de coluna** na barra de ferramentas.
3. Na caixa de diálogo **Configurações de colunas**, digite um nome para a nova configuração.



4. Selecione os atributos de inventário na lista e adicione-os à lista Colunas, clicando em **Adicionar às colunas**. Lembre-se de selecionar atributos que ajudarão a identificar os dispositivos na lista de dispositivos ou retornados pela consulta.
5. (Opcional) Você pode personalizar a forma e o lugar onde as colunas aparecerão na tela de rede editando diretamente o cabeçalho, álias e campos de seqüência de um componente; ou através da remoção e da mudança do componente selecionado para cima ou para baixo na lista, utilizando os botões disponíveis.

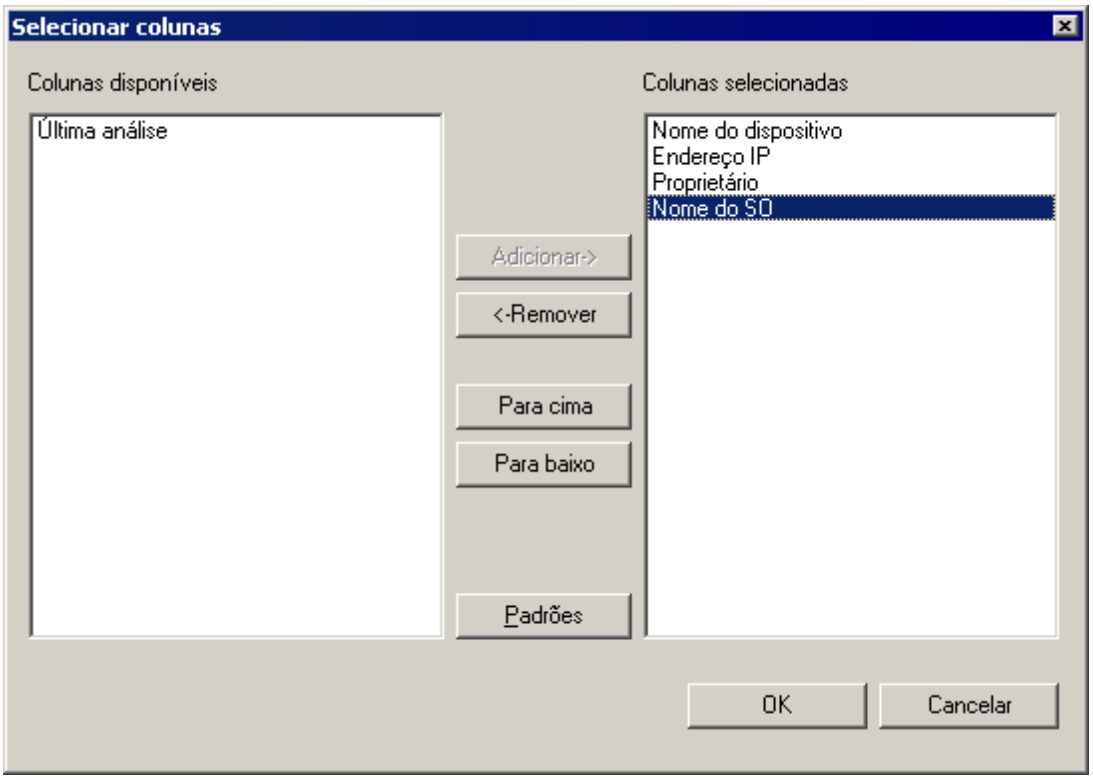
6. (Opcional) Você pode especificar dados de qualificação mais precisos para os componentes de software. Selecione o componente de software, clique no botão **Qualificar** e selecione um valor de chave primária na lista de valores disponíveis. Para ver mais informações, consulte "Especifique a opção de qualificação com os componentes de software" na página 17.
7. Clique em **OK** para salvar o conjunto de colunas.

Exibição de colunas

Se após definir certos atributos de inventário, você decidir ocultar ou mover a posição de uma coluna na Tela de rede, você pode usar o menu de atalhos para exibir a caixa de diálogo **Selecionar colunas** .

Para mudar ou ocultar as colunas exibidas

1. Clique com o botão direito em qualquer dispositivo na lista de resultados da Tela de rede.
2. Selecionar **Colunas...**
3. Use os botões **Adicionar ->**, **<-Remove**r, **Mover para cima**, ou **Mover para baixo** para organizar as colunas.
4. Clique em **OK**.



Você também pode voltar a exibir as colunas de acordo com a configuração original clicando em **Padrões**.

Aplicar conjuntos de colunas a grupos de dispositivos e consultas

Após ter criado um conjunto de colunas, arraste-o para um grupo ou subgrupo de dispositivos ou para um objeto de consulta específico em um grupo ou subgrupo de consultas. A lista de dispositivos ou a lista de resultados da consulta, exibe os dados de inventário especificados pelo conjunto de colunas selecionado no painel direito da Tela de rede.

Observe que para as listas de dispositivos, uma vez que o conjunto de colunas é aplicado a um grupo ele persiste mesmo quando você seleciona grupos diferentes de dispositivos. Entretanto, no caso das lista de resultados de consulta, o conjunto de colunas deve ser reaplicado ao mover entre as várias consultas.

Clique com o botão direito num conjunto de colunas para acessar seu menu de atalho e realizar tarefas comuns, assim como ver e editar suas propriedades. O menu de atalho contém as seguintes opções:

- Adicionar a um novo grupo
- Adicionar a um grupo existente
- Membro de grupo
- Definir como padrão
- Exibir como relatório:
- Exportar como CSV
- Copiar
- Excluir
- Renomear
- Propriedades
- Inf.
- Exportar
- Copiara para outro(s) núcleo(s)
- Sinc. automática
- Colunas

Especifique a opção de qualificação com os componentes de software

Ao criar conjuntos de colunas que contêm componentes de software, você pode especificar um critério de qualificação para os componentes de software, escolhendo um valor de chave primária específico. O critério de qualificação do software permite identificar mais precisamente os dados a serem procurados pela consulta e mostrados na coluna do componente de software. Por exemplo, você pode configurar o conjunto de colunas para mostrar as informações da versão de apenas um aplicativo específico selecionando o nome do arquivo executável desse aplicativo como critério de qualificação.

Para especificar um critério de qualificação de componente de software, selecione o componente de software na lista Colunas, clique no botão **Qualificar** e selecione um valor da lista de valores de chave primária disponíveis.

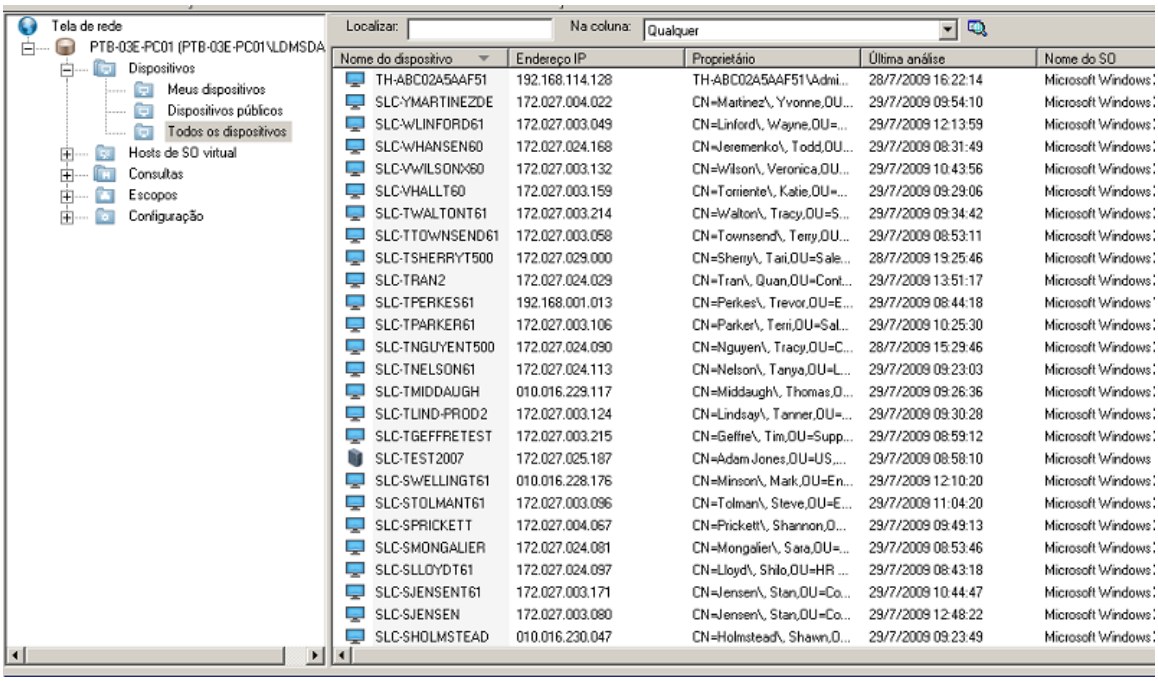
Sobre a caixa de diálogo Configurações de colunas

Esta caixa de diálogo contém as seguintes opções:

- **Nome:** Identifica a configuração de coluna.
- **Atributos de inventário:** relaciona cada um dos objetos de inventário e os atributos analisados no banco de dados núcleo. Amplie ou reduza os objetos, clicando na caixa à esquerda do objeto.
- **Adicionar às colunas:** transfere o atributo de inventário selecionado para a lista de colunas. Se você selecionar um componente inteiro de inventário, todos os atributos de inventário contidos nesse componente serão adicionados à lista de colunas.
- **Colunas:** Relaciona os atributos de inventário na ordem em que serão exibidos na Tela de rede, da esquerda para a direita.
- **Qualificar:** Permite especificar um critério preciso de qualificação de dados para o componente de software selecionado. Para obter mais informações, consulte "Especifique a opção de qualificação com os componentes de software" na página 17.
- **Remover:** remove o atributo selecionado da lista.
- **Mover para cima:** move o atributo selecionado uma posição para cima.
- **Mover para baixo:** move o atributo selecionado uma posição para baixo.
- **OK:** salva a atual configuração de coluna e fecha a caixa de diálogo.
- **Cancelar:** fecha a caixa de diálogo sem salvar nenhuma alteração.

Exibir dispositivos gerenciados

Os dispositivos que estiverem executando os agentes LANDesk aparecem automaticamente no grupo **Todos os dispositivos** quando são analisados no banco de dados núcleo pelo analisador de inventário. Normalmente, essa análise é feita pela primeira vez durante a configuração inicial de agente do dispositivo. Assim que o dispositivo é analisado e seu relatório de inventário foi enviado para o banco de dados núcleo, ele passa a ser considerado um dispositivo gerenciado. Em outras palavras, o cliente agora pode ser gerenciado pelo servidor núcleo. Para obter mais informações sobre a configuração de dispositivos, consulte ""Configuração de agentes" na página 99".

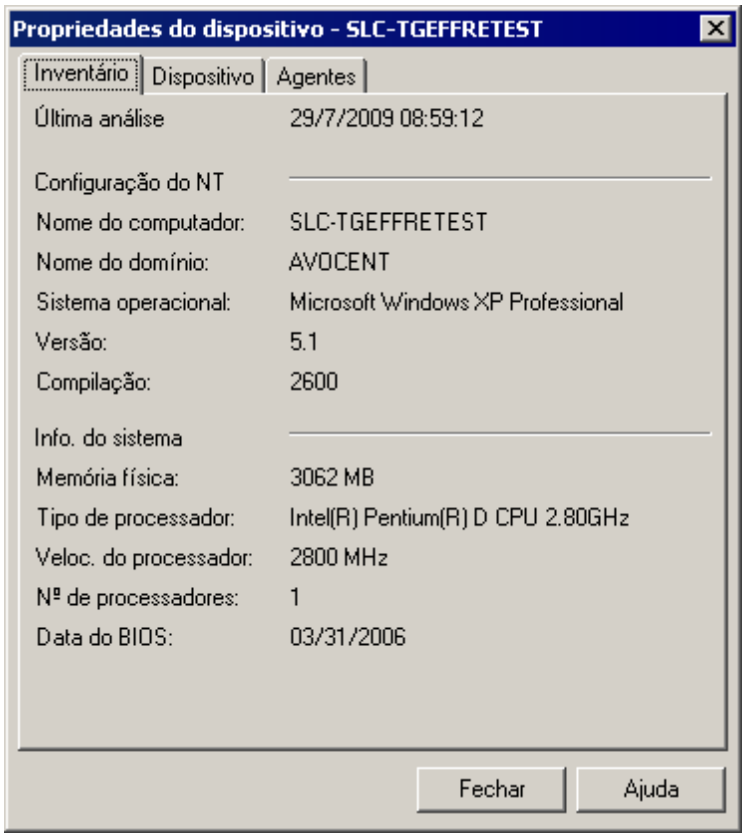


Pelo fato de o grupo **Todos os dispositivos** ser preenchido automaticamente por meio de uma análise de inventário, talvez não seja preciso descobrir dispositivos manualmente. Entretanto, para descobrir dispositivos que ainda não estão no banco de dados núcleo, você pode efetuar uma varredura da rede em busca de dispositivos, usando a ferramenta Descoberta de dispositivos não gerenciados. Para obter mais detalhes, consulte "Como ver o resumo de inventário" na página 149.

Quando conectado a um determinado servidor núcleo, o administrador pode ver todo dispositivo gerenciado por esse servidor núcleo. Outros usuários estão restritos e só podem ver os dispositivos contidos no escopo que lhe foi atribuído (um escopo é baseado em uma consulta do banco de dados ou em um local de diretório). Para obter mais informações, consulte "Gerenciamento de usuários" na página 38.

Exibir propriedades do dispositivo

Na Tela de rede console, você pode exibir rapidamente informações sobre um dispositivo clicando com o botão direito do mouse no dispositivo da lista de dispositivos e selecionando **Propriedades**.



Caixa de diálogo Propriedades do dispositivo

Use essa caixa de diálogo para exibir informações úteis sobre o dispositivo selecionado. A caixa de diálogo possui três guias: **Inventário**, **Dispositivo** e **Agentes**. Clique em cada um para exibir as informações relacionadas.

Sobre a guia Inventário

A guia **Inventário** contém um resumo dos dados de inventário do dispositivo. Para obter mais detalhes, consulte "Como ver o resumo de inventário" na página 149

Guia Dispositivo

A guia **Dispositivo** contém informações básicas sobre um dispositivo como, sua localização e sua identidade na rede. Essa guia também aparece quando você insere manualmente um dispositivo (no menu de atalho do grupo **Todos os dispositivos**, clique em **Inserir novo computador**).

- **Dispositivo:**
  - **Nome:** nome do dispositivo que aparece no banco de dados núcleo e na tela de rede. Se você inserir um dispositivo manualmente, você pode criar um nome amigável. Se não for digitado nada aqui, o nome padrão do dispositivo será o nome Windows do computador.
  - **Tipo:** Tipo de dispositivo, como por exemplo, Windows Server 2008 ou XP Workstation.
- **Rede:**
  - **Nome IP:** nome Windows do computador do dispositivo.
  - **Endereço IP:** o endereço IP atribuído ao dispositivo.
  - **Endereço físico:** o endereço físico do dispositivo.

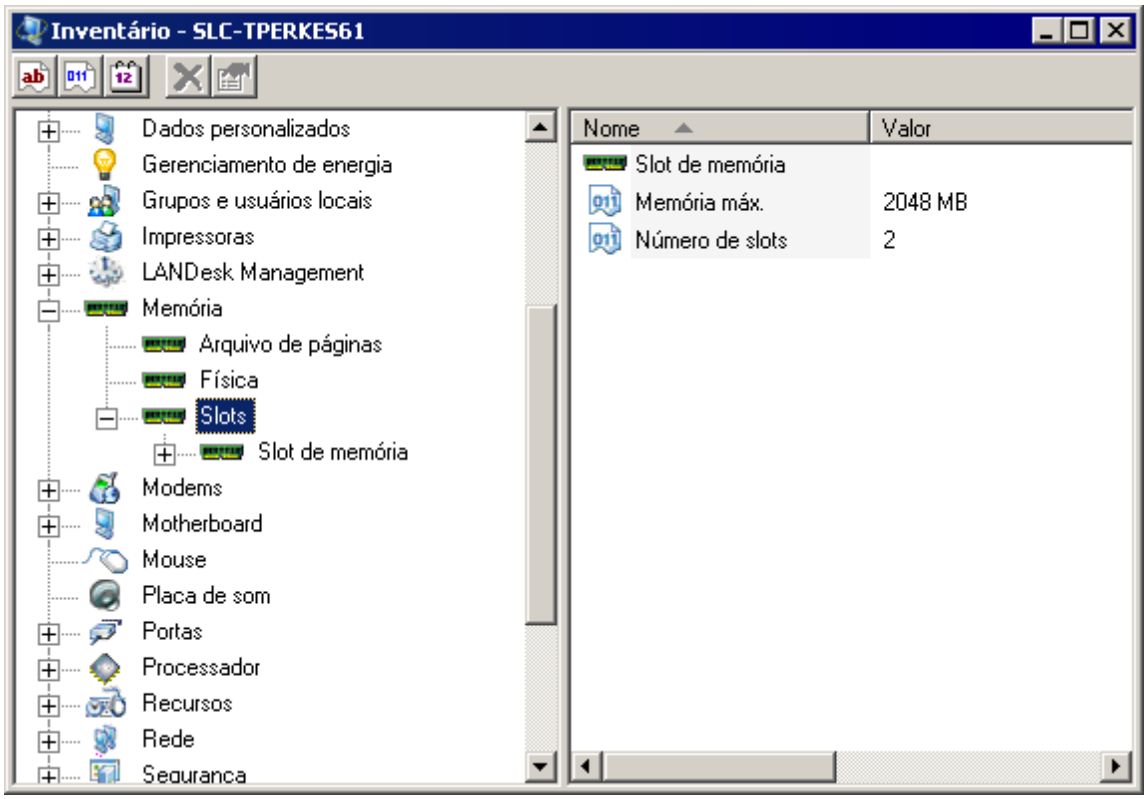
Sobre a guia Agentes

A guia **Agentes** contém informações sobre o status atual dos agentes e as configurações de controle remoto do dispositivo.

- **Status do CBA (Common Base Agent)** Indica se o agente LANDesk padrão (Common Base Agent) está carregado no dispositivo.
- **Status do inventário e monitoramento em tempo real:** Indica se o agente de inventário e monitoramento em tempo real está sendo executado no dispositivo.
- **Status do agente de controle remoto:** Indica se o agente de controle remoto está carregado no dispositivo. Se esse agente não estiver carregado no dispositivo, as operações de controle remoto (como transferência de arquivos e bate-papo) não estarão disponíveis.
- **Tipo de segurança:** indica o modelo de segurança de controle remoto usado para o dispositivo. As opções são: Modelo local, modelo segurança do Windows NT/local e modelo baseado em certificado/local.
- **Permitir:** mostra as operações de controle remoto permitidas no dispositivo. Essas operações foram habilitadas pela configuração de agentes do dispositivo.
- **Configurações:** indica como o controle remoto funciona quando você tenta interagir com o dispositivo.

Dados de inventário

Veja outras informações mais detalhadas sobre o dispositivo em seus dados de inventário. Você pode ver um grande volume de informações do inventário clicando duas vezes no nome de dispositivo no painel de resultados da Tela de rede.



Configuração de alertas de monitoramento de dispositivos

Se você quiser que o monitoramento de dispositivo o notifique quando dispositivos gerenciados ficarem online ou offline, você precisa primeiro configurar um conjunto de regras de alerta que tenha ações adicionais (como receber um e-mail quando o alerta for enviado).

Para configurar os alertas de monitoramento de dispositivos

1. Clique em **Ferramentas > Configuração > Alerta**.
2. Na árvore **Alertas**, expanda o item **Conjuntos de regras de alerta**.
3. Clique com o botão direito em **Conjuntos de regras de alerta do núcleo** e clique em **Editar**.
4. No painel à esquerda **Conjunto de regras de alerta** da janela **Conjunto de regras**, clique em **Alertas**.
5. No painel **Alertas**, sob a pasta **Padrão**, clique em **Monitor de dispositivos**.
6. No painel direito, clique em **Regras > Adicionar**.
7. Arraste o alerta **Conectivity do sistema do monitor de dispositivos** para os **Alertas** na parte inferior da página.
8. No painel **Conjunto de regras de alerta** da esquerda na janela **Conjunto de regras**, clique em **Ações** e arraste qualquer ação adicional que quiser para o compartimento **Ações**. Como padrão a configuração do identificador do log de alerta do núcleo é a ação. Você pode escolher enviar um e-mail ou uma interceptação de SNMP, ou abra um arquivo executável no núcleo quando o alerta for recebido. (Você precisa definir cada ação, tal como especificar para onde enviar alertas por e-mail.)

9. No painel à esquerda **Conjunto de regras de alerta** da janela **Conjunto de regras** clique em **Hora** e arraste **Sempre** ao compartimento **Hora**.
10. Clique no botão **OK** próximo aos compartimentos.
11. No painel **Ações** à direita, clique em **Publicar**.
12. No painel **Conjunto de regras de alerta** à esquerda, clique em **Resumo das regras** e clique duas vezes na regra que você criou.
13. No diálogo exibido, marque a caixa **Funcionamento** se desejar que o status de funcionamento de um dispositivo no console mude quando estiver online/offline, e em seguida, clique em **OK** para fechar o diálogo.
14. Clique em **Publicar** para publicar qualquer mudança que você fez no diálogo e feche a jenela **Conjunto de regras**.

NOTA: Quando são definidas, as configurações de alerta aplicam-se a todos os dispositivos que estão sendo monitorados.

Monitoramento de dispositivos para conectividade de rede

O monitoramento de clientes permite monitorar periodicamente a conectividade de qualquer um dos dispositivos gerenciados.

As configurações de ping são específicas para o dispositivo selecionado. Quando um dispositivo para de responder a um ping (quando ele fica offline), é adicionado um alerta de notificação ao login no servidor núcleo. Se você quiser ser notificado com outra ação de alerta, como receber um e-mail quando um dispositivo fica offline, você pode configurar um alerta no conjunto de regras de alerta do núcleo.

Para monitorar conectividade para dispositivos gerenciados

1. Clique em **Configurar > Monitoramento de dispositivos**.
2. Clique em **Adicionar**. Selecione um ou mais dispositivos que você deseja monitorar e, em seguida, clique em **Adicionar**.
3. Especifique a configuração **Frequência de ping**, o número de tentativas e o limite de tempo.
4. Clique em **OK**.

Sobre a caixa de diálogo Configurar o monitoramento de dispositivos

Use essa caixa de diálogo para configurar as seguintes opções de monitoramento de dispositivos.

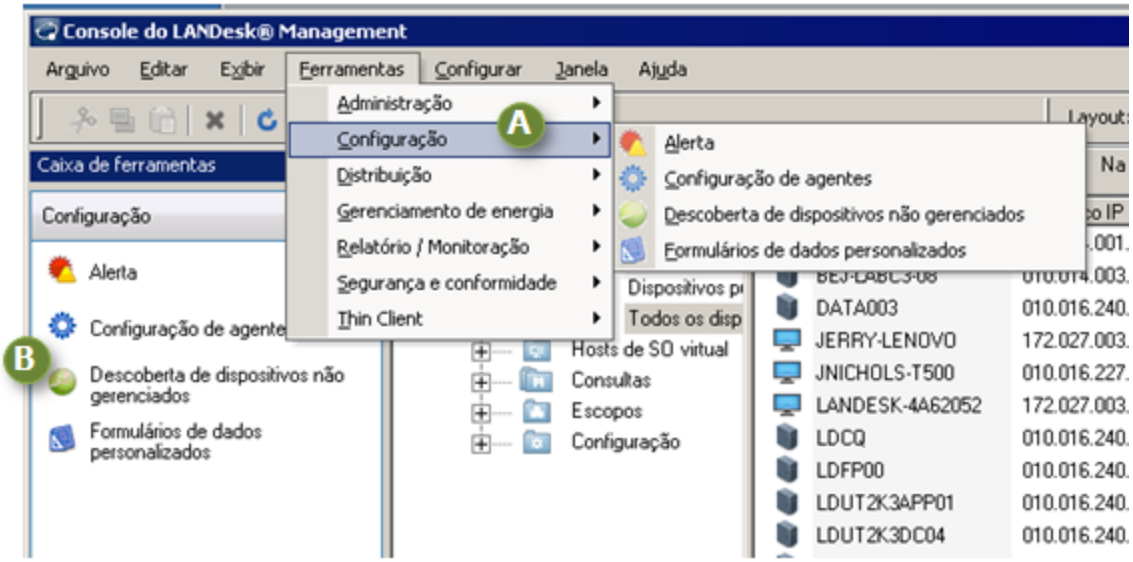
- **Monitorar estes dispositivos:** mostra os dispositivos que estão sendo monitorados.
- **Adicionar:** abre a caixa de diálogo **Adicionar dispositivos monitorados** onde você poderá procurar e selecionar os dispositivos gerenciados que deseja monitorar.
- **Remover:** exclui o dispositivo selecionado da lista.
- **Freqüência de ping:** Controla quando e como a operação de ping ocorre. Essas configurações podem ser aplicadas aos dispositivos individualmente.
    - **Ping a cada:** agenda um ping periódico para o intervalo em minutos especificado.
    - **Agendar diariamente às:** agenda um ping diário em um horário específico.
    - **Novas tentativas:** especifica o número de novas tentativas de ping.

- **Tempo limite:** especifica o número de segundos até as novas tentativas de ping atingirem o tempo limite.

- **OK:** Salva as alterações e fecha a caixa de diálogo.
- **Cancelar:** Fecha a caixa de diálogo sem salvar as alterações.

Acessar ferramentas do console

As ferramentas do console estão disponíveis em ambos, o **Menu de ferramentas (A)** e a **Caixa de ferramentas (B)**. Para ativar a Caixa de ferramentas, clique em **Exibir > Caixa de ferramentas**. Para economizar espaço no console, entretanto, você pode optar por não habilitar a Caixa de ferramentas e apenar selecionar ferramentas do menu de Ferramentas.



***A** Menu de ferramentas, **B** Painel caixa de ferramentas*

O administrador Management Suite pode ver todas as ferramentas tanto no menu **Ferramentas** como na **Caixa de ferramentas**. Os outros usuários Management Suite podem ver apenas as ferramentas e recursos permitidos pelos seus direitos atribuídos. As ferramentas que dependem de permissões que não foram concedidas a um usuário não são exibidas no menu Ferramentas nem na Caixa de ferramentas quando este usuário está conectado ao console. Por exemplo, se o usuário não tiver o direito a "Gerenciamento de energia", a ferramenta Gerenciamento de energia não aparecerá no menu **Ferramentas** nem na **Caixa de ferramentas**.

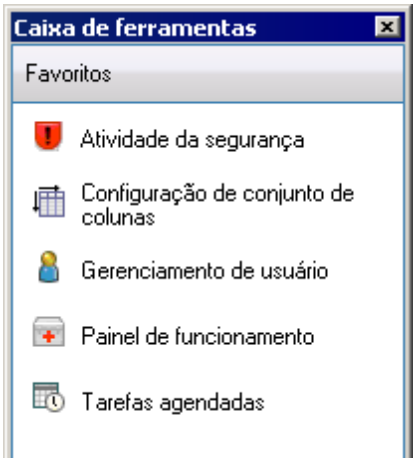
Ao clicar no nome de uma ferramenta, sua janela é aberta no console, abaixo da Tela de rede.

As janelas de ferramentas podem ser redimensionadas, encaixadas, flutuantes, ocultas e fechadas. É possível abrir, simultaneamente, várias janelas de ferramentas, encaixá-las ou torná-las flutuantes. Para obter mais informações, consulte "Mover e redimensionar janelas de ferramentas" na página 24.

Favoritos

Se você acredita que usa certas ferramentas com mais frequência do que outras, você pode configurar uma caixa de ferramentas favorita clicando com o botão direito em qualquer ferramenta na caixa de ferramentas e selecionando "Exibir em Favoritos". Em seguida, você pode acessar seus Favoritos a partir do botão Favoritos na parte inferior do painel da Caixa de ferramentas.

Exibir/ocultar imagens



Mover e redimensionar janelas de ferramentas

O console permite que você abra quantas ferramentas quanto necessárias, além de movê-las para dentro e fora da janela principal do console.

NOTA: Você pode salvar os layouts de console criados e os de sua preferência para determinadas tarefas de gerenciamento, além de restaurar um layout salvo sempre que precisar. Para obter mais informações, consulte "Salvar layouts de console" na página 29.

Quando você abre várias janelas de ferramentas, elas são dispostas em uma única janela. A janela de ferramentas ativa é exibida na parte superior da tela, com uma guia para cada ferramenta aberta em execução disposta ao lado ou na parte inferior. Clique em uma guia para exibir a janela dessa ferramenta.

Encaixar janelas de ferramentas

Você pode "encaixar" uma janela de ferramenta arrastando-a a uma das bordas do console. A janela está em um estado encaixado se estiver anexada a uma das bordas do console. As janelas podem ser encaixadas horizontal ou verticalmente no console.

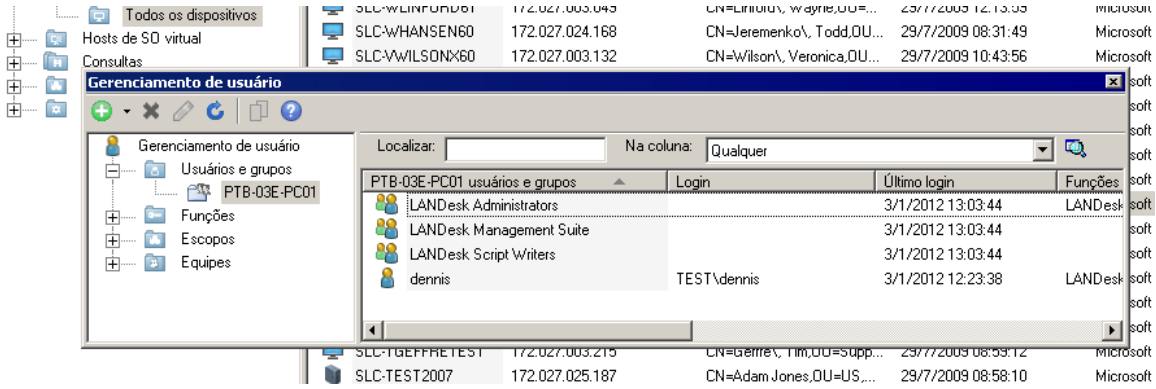
Para encaixar uma janela de ferramenta

1. Clique na barra de título da janela e arraste-a para uma das bordas do console
2. Quando o retângulo de encaixe (borda esmaecida da janela) for exibido, indicando que a janela será encaixada, solte o botão do mouse. A janela será anexada a essa borda do console.

Flutuar janelas de ferramentas

Você também pode também desencaixar a janela de ferramentas e arrastá-la (usando sua barra de título) para que possa flutuar para outro local dentro ou fora da área do console. Ferramentas flutuantes podem ser arrastadas ou redimensionadas para que seja possível movê-las temporariamente para fora do caminho e proporcionar mais espaço para trabalhar em outras tarefas. Ao arrastar a janela de ferramentas, as guias das outras ferramentas abertas também são arrastadas. Clique duas vezes sobre a ferramenta para retorná-la ao lugar padrão. Ou arraste-a de volta a sua posição e solte-a ao ver o retângulo de encaixe (cinza) no local correto.

Exibir/ocultar imagens



Observe que apenas as janelas de ferramentas (as que podem ser acessadas pelo menu Ferramentas ou pela Caixa de ferramentas) podem existir como janelas encaixadas, flutuantes ou com guias. A janela da Tela de rede pode ser redimensionada, mas não pode ser colocada em guias com outras janelas, flutuar fora do console, nem fechada.

Se você minimizar e, em seguida, restaurar a janela principal do console, todas as janelas encaixadas e flutuantes, inclusive as janelas em guias, também serão minimizadas e restauradas.

Auto-ocultar janelas de ferramentas

As janelas de ferramentas também suportam o recurso Auto-ocultar. Auto-ocultar é um botão tipo tachinha, localizado no canto superior direito de uma janela, que permite mantê-la no lugar ou ocultá-la.

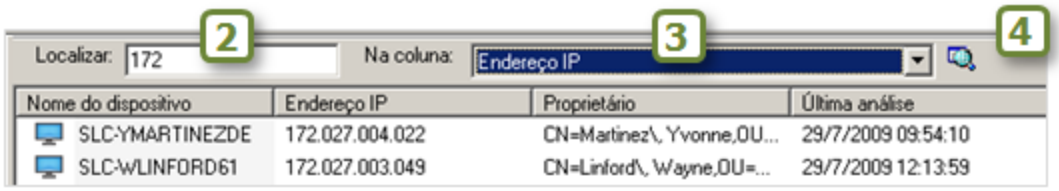
Quando o botão está ativado (ou seja, quando a tachinha está apontando para baixo), a janela é fixada no lugar e o recurso Auto-ocultar fica temporariamente desativado. Quando o botão está desativado (ou seja, a tachinha está apontando para a esquerda), a janela entra no modo Auto-ocultar quando o cursor é movido para fora da janela. O Auto-ocultar minimiza e encaixa a janela ao longo de uma das bordas do console e exibe uma guia em seu lugar.

As janelas de ferramentas também são compatíveis com o recurso Auto-ocultar.

Procure por itens com a barra Localizar

A barra Localizar aparece em uma barra de ferramentas sempre que fizer sentido para o usuário procurar um item específico em uma lista correspondente. Por exemplo, sempre que uma lista de itens for mostrada na parte superior ou inferior do console, a barra Localizar está incluída nesta exibição para facilitar a localização de um item específico na lista correspondente.

Um exemplo pode ser útil. Considere uma organização com 10.000 nós relacionados no banco de dados. Um usuário liga para pedir assistência e o membro da equipe do helpdesk precisa encontrar o dispositivo no console. O membro do helpdesk pode pedir o nome de login do usuário ou o nome do computador ou quaisquer outras informações específicas do usuário e localize a entrada exata entre as 10.000 entradas em um ou dois segundos.



***Passo 2** Encontre a caixa de texto, **3** Na lista Coluna, **4** Botão pesquisar*

Para pesquisar um item com a barra Localizar

1. Selecione o grupo **Todos os dispositivos**. A barra **Localizar** aparece na parte superior da lista.
2. Na caixa de texto **Localizar**, digite o texto que deseja pesquisar.
3. Na lista **Na coluna**, selecione a coluna na qual você deseja pesquisar
4. Clique no botão da barra de ferramentas **Pesquisar**.

A lista resultante exibe apenas os itens que correspondem aos seus critérios de pesquisa.

Opções da barra de ferramentas

O console inclui uma barra de ferramentas que permite acessar, com um único clique, as operações comuns da tela de rede e algumas opções básicas de configuração do console. Os botões da barra de ferramentas ficam esmaecidos quando um item da Tela de rede que não é compatível com a operação é selecionado.

Botões da barra de ferramenta do console

- **Recortar:** Remove itens da Tela de rede e armazena-os temporariamente na área de transferência. Se recortar um item acidentalmente, use o comando Colar para restaurá-lo. Você deve restaurar o item excluído antes de executar qualquer outro comando.
- **Copiar:** Copia itens de um local para outro na Tela de rede.
- **Colar:** cola os itens recortados ou copiados.
- **Excluir:** remove o item permanentemente. Não é possível restaurar itens excluídos da tela de Visualização de rede.
- **Atualizar:** Atualiza o grupo ou item selecionado na Tela de rede. Também é possível ampliar e reduzir um grupo para atualizar seus itens. Você pode clicar em **Exibir > Atualizar** para atualizar o item selecionado na Tela de rede.
- **Atualizar escopo:** Atualiza o grupo ou item selecionado na tela de rede, com base no escopo do usuário acessado no momento (conforme definido na ferramenta Usuários). Os escopos são atualizados quando os usuários acessam ou quando um usuário de console com privilégios administrativos clica neste botão.
- **Layout:** mostra os layouts das janelas salvos. Selecione um layout na lista suspensa para restaurar o console a essa configuração de layout. Se desejar salvar o layout atual, clique no botão **Salvar layout atual**.
- **Núcleo:** Mostra os servidores núcleo aos quais havia conectado antes (que os faz aparecer nesta lista). Você pode selecionar um servidor núcleo na lista ou digitar o nome de um servidor núcleo e pressionar **Enter**. Esse servidor núcleo é procurado na rede e, se encontrado, você é avisado para iniciar a sessão com um nome de usuário e senha válidos.

Menus de atalho

Menus de atalho (contexto) estão disponíveis para todos os itens do console, inclusive grupos, dispositivos, consultas, tarefas agendadas, scripts, relatórios etc. Os menus de atalho proporcionam acesso rápido às tarefas comuns e às informações críticas de um item.

Para ver o menu de atalho de um item, selecione o item e clique nele com o botão direito.

Opções disponíveis no menu atalho

As opções que aparecem em um menu de atalho do dispositivo, assim como as opções que estão desativadas ou escurecidas, podem diferir dependendo da plataforma do dispositivo e dos agentes do LANDesk que estiverem instalados nos dispositivos.

Por exemplo, ao clicar com o botão direito do mouse em um dispositivo gerenciado na Tela de rede, o seu menu de atalho exibirá normalmente as seguintes opções:

- **Inventário:** Mostra todos os dados de inventário do dispositivo no banco de dados núcleo.
- **Histórico do inventário:** Exibe mudanças nos dados de inventário baseado nos atributos que você selecionou para rastreamento. O histórico do inventário pode ser impresso ou exportado para um arquivo .CSV.
- **Controle remoto:** Abre uma sessão de controle remoto com o dispositivo.
    - **Chat:** Abre uma sessão de sessão de bate-papo remoto com o dispositivo.
    - **Transferência de arquivo:** Abre a caixa de diálogo Transferência de arquivos, pela qual é possível transferir arquivos de e para o dispositivo.
    - **Execução remota:** Permite procurar e executar um arquivo de lote ou um aplicativo no dispositivo.
    - **Reinicialização:** Permite que você reinicie o dispositivo.
- **Ativar:** Ativa remotamente um dispositivo cujo BIOS suporta a tecnologia Wake on LAN.
- **Desligar:** Desliga o dispositivo remotamente.
- **Análises de inventário:** Executa uma varredura de inventário no dispositivo.
- Gerencia variáveis:
- Histórico do provisionamento:
- **Tarefas agendadas e diretivas:** Exibe as atuais tarefas agendadas e diretivas de gerenciamento de aplicativos do dispositivo.
- **Adicionar a um novo grupo:** adiciona uma cópia do dispositivo em um novo grupo definido pelo usuário no grupo **Meus dispositivos**. É solicitado que você digite um nome para o novo grupo.
- **Adicionar a um grupo existente:** Permite a seleção do grupo ao qual você deseja adicionar uma cópia do dispositivo.
- **Membro de grupo:** Exibe todos os grupos dos quais o cliente é um membro atualmente.
- **Executar relatório de inventário:** abre a caixa de diálogo Relatórios, no qual é possível selecionar um relatório de uma lista para execução no dispositivo. Clique duas vezes em um nome de relatório para executá-lo.

- **Atualização das definições do Agente Watcher:** Abre a caixa de diálogo Atualização das definições do Agent Watcher onde você pode habilitar/desabilitar o monitoramento em tempo real de serviços e agentes específicos LANDesk, escolher uma configuração do Agent Watcher ou configurar uma nova e especificar um intervalo de tempo para verificar as mudanças na definição selecionada.
- **Informações de segurança e patch:** Abre a caixa de diálogo Informações de segurança e patch que exibe dados de análise detalhada de vulnerabilidade e de remediação para o dispositivo, inclusive vulnerabilidades detectadas e outras ameaças à segurança, patches instalados e histórico de reparação.
- **Análise de segurança/conformidade agora:** Abre uma caixa de diálogo que permite que você selecione uma configuração de análise e reparo. Clique em **OK** para executar uma análise de segurança imediatamente no dispositivo.
- **Análise de Antivírus agora:** Abre um diálogo que permite selecionar configurações de antivírus, a seguir você clica em **OK** para executar uma análise de antivírus imediata no dispositivo.
- **Gerenciar usuários e grupos locais:** abre o diálogo Usuários e grupos locais e permite gerenciar remotamente os usuários e dispositivos locais de um dispositivo Windows.
- **Recortar:** remove itens de um grupo definido pelo usuário. Não é possível recortar itens de grupos "Todos".
- **Copiar:** cria uma cópia do item que você deseja adicionar em outro grupo.
- **Colar:** insere o item recortado ou copiado em um grupo definido pelo usuário.
- **Remover:** remove o item de um grupo definido pelo usuário.
- **Excluir:** Exclui o item do grupo "Todos" e de qualquer outro grupo do qual for membro no momento.
- **Propriedades:** mostra o resumo de inventário do dispositivo, as informações de dispositivo, o status de agente e as configurações de controle remoto.

Este tópico da ajuda não aborda todos os menus de atalho possíveis de cada tipo de item. Clique com o botão direito em qualquer item para ver as opções disponíveis.

NOTA: Se a sua firewall bloquear os pacotes UDP
Se você gerencia dispositivos através de uma firewall que bloqueia pacotes UDP, não será possível usar os seguintes recursos de menu de atalho desses dispositivos: **Ativar**, **Desligar**, **Reinicializar** e **Análise de inventário**.

Barra de status

A barra de status na parte inferior do console contém as seguintes informações (da esquerda para a direita):

Elementos da barra de status

- O número de itens selecionados em uma lista
- O nome e o status do trabalho atual
- Nome do usuário atualmente conectado

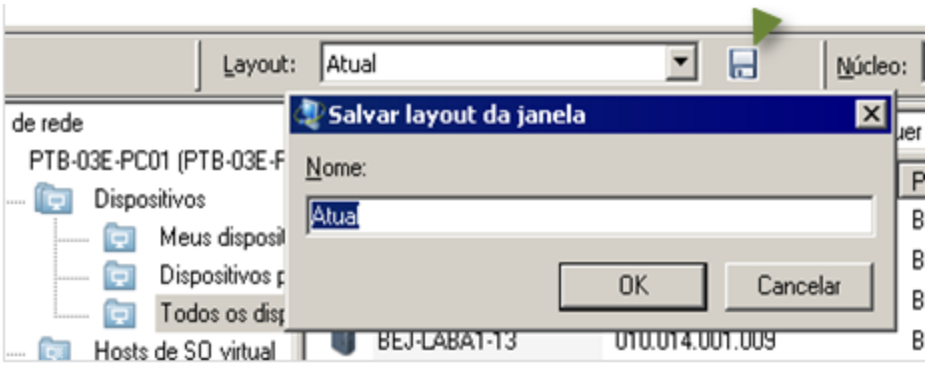
Salvar layouts de console

Os layouts são configurações gravadas do console, isto é, a posição e o tamanho da Tela de rede, a Caixa de ferramentas e todas as janelas de ferramentas abertas. Você pode usar layouts de janelas para salvar e restaurar configurações personalizadas do console que sejam especialmente úteis para certas tarefas ou usuários.

Para alterar o layout do console, selecione um layout gravado na lista **Layout** da barra de ferramentas principal.

Para salvar o layout atual:

1. Configure a interface do console da maneira desejada.
2. Clique no botão **Disco** ao lado da lista **Layout** da barra de ferramentas.
3. Digite um nome exclusivo para o layout.
4. Clique em **OK**.



Sobre a caixa de diálogo Gerenciar layouts de janelas

Use esta caixa de diálogo para gerenciar layouts de janelas gravados e para redefinir a janela do console para o layout anterior.

- **Layouts salvos:** relaciona todos os layouts salvos.
- **Redefinir:** restaura a janela do console ao layout anterior.
- **Excluir:** remove o layout selecionado.
- **Renomear:** permite alterar o nome do layout selecionado.

Modificar a conexão do servidor núcleo

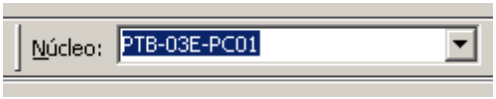
O console permite exibir e gerenciar o conteúdo de qualquer banco de dados associado a um servidor núcleo ao qual você pode se conectar na rede. Isso permite criar bancos de dados para locais diferentes, unidades organizacionais ou redes internas lógicas.

Você pode conectar-se somente a um servidor núcleo de cada vez.

Para mudar as conexões com o servidor núcleo

1. Selecione um servidor núcleo na lista suspensa **Núcleo**, localizada no lado direito da barra de ferramentas do console. Ou, digite o nome de um servidor núcleo na caixa de texto **Núcleo** e

pressione **Enter**.



O servidor procurado na sua rede. Se ele for encontrado, você será solicitado a fazer logon na caixa de diálogo padrão de Login.

2. Digite o nome de usuário e a senha.

Siga as regras normais do Windows para login remoto (ou seja, se o usuário estiver no mesmo servidor núcleo, basta digitar o nome do usuário; se o usuário for um usuário do domínio, digite o nome do domínio\nome de usuário).

Após conectar-se a um servidor núcleo, o nome do servidor é automaticamente adicionado à lista **Núcleo** na barra de ferramentas.

É possível também acessar rapidamente como outro usuário no núcleo atual. Para fazer isso, clique na lista **Núcleo** e, sem mudar o nome do núcleo, pressione Enter.

Visualização de dados com o inspetor

O inspetor de Conjunto de Gerência de LANDesk exibe detalhes sobre itens no console de LANDesk. Use o inspetor rapidamente achar informações sobre dispositivos administrados, os grupos, perguntas, configurações de segurança, e muitos mais itens.

Os inspetores são definidos para muitos itens normais. Por exemplo, você pode examinar dispositivos administrados, tarefas programadas, vulnerabilidades, e o servidor núcleo.

Os direitos de usuário exigiram ver o inspetor

Para exibir o inspetor, um usuário deve ter o direito correto designado em administração de Papel-Baseou. O Inspetor correto tem só uma opção, Vista, que podem ser capacitados para um usuário. Se um usuário não tem este direito, o Auto inspetor e opção de contexto-menu para o inspetor não são visíveis.

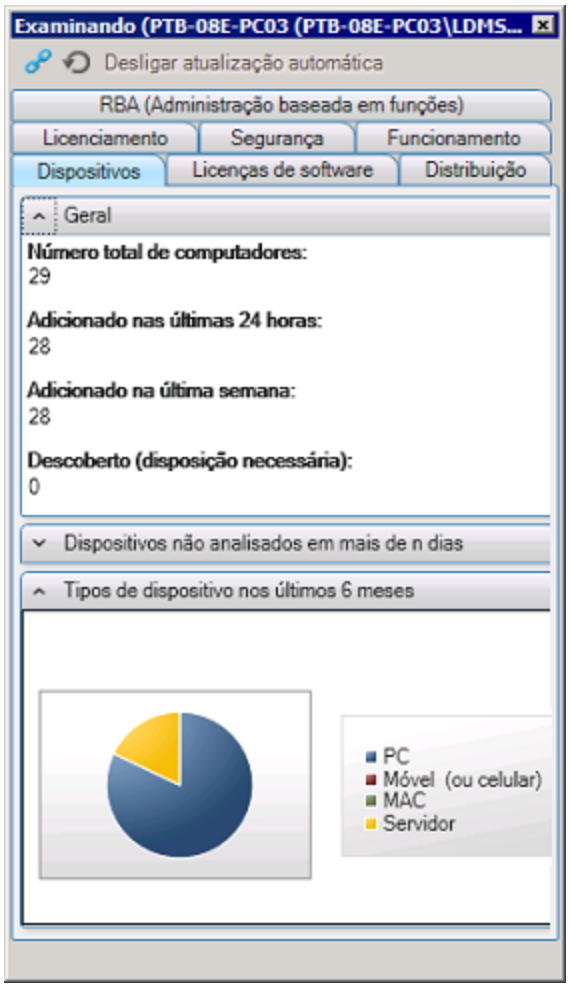
Para obter mais informações sobre a administração baseada em funções, consulte "Gerenciamento de usuários" na página 38.

Abrir uma janela de inspetor

Há duas maneiras de ver dados em uma janela de inspetor:

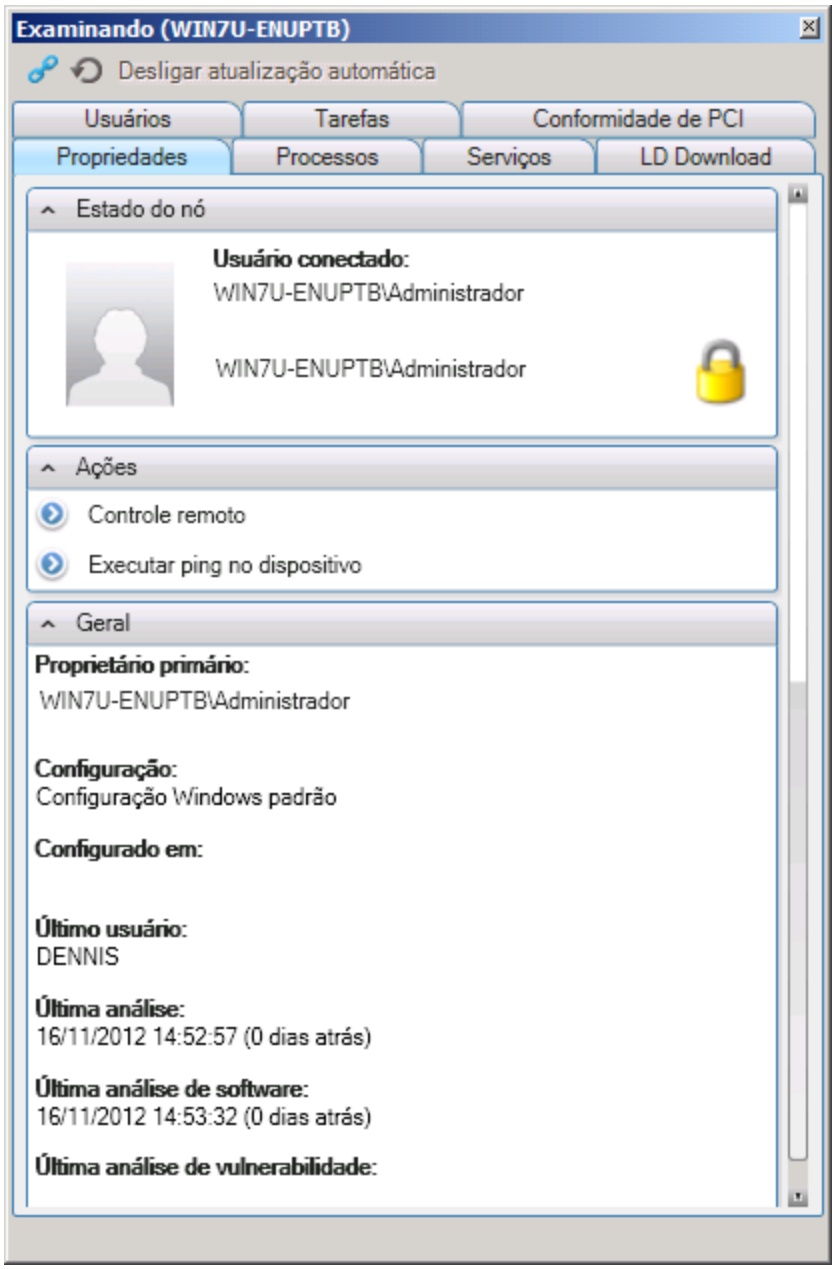
- Ligue o Auto inspetor (**Vista de clique> Auto examina**). Isto abre uma janela que exibe dados sempre que você clicar em um item. Cada vez você clica outro item, esse dados do item aparecem na Auto janela de inspetor.
- Clique com o botão direito em um item e selecione **Inspecionar**. Uma nova janela de inspetor abre com dados para esse item.

As janelas de inspetor abrem separadamente do console.

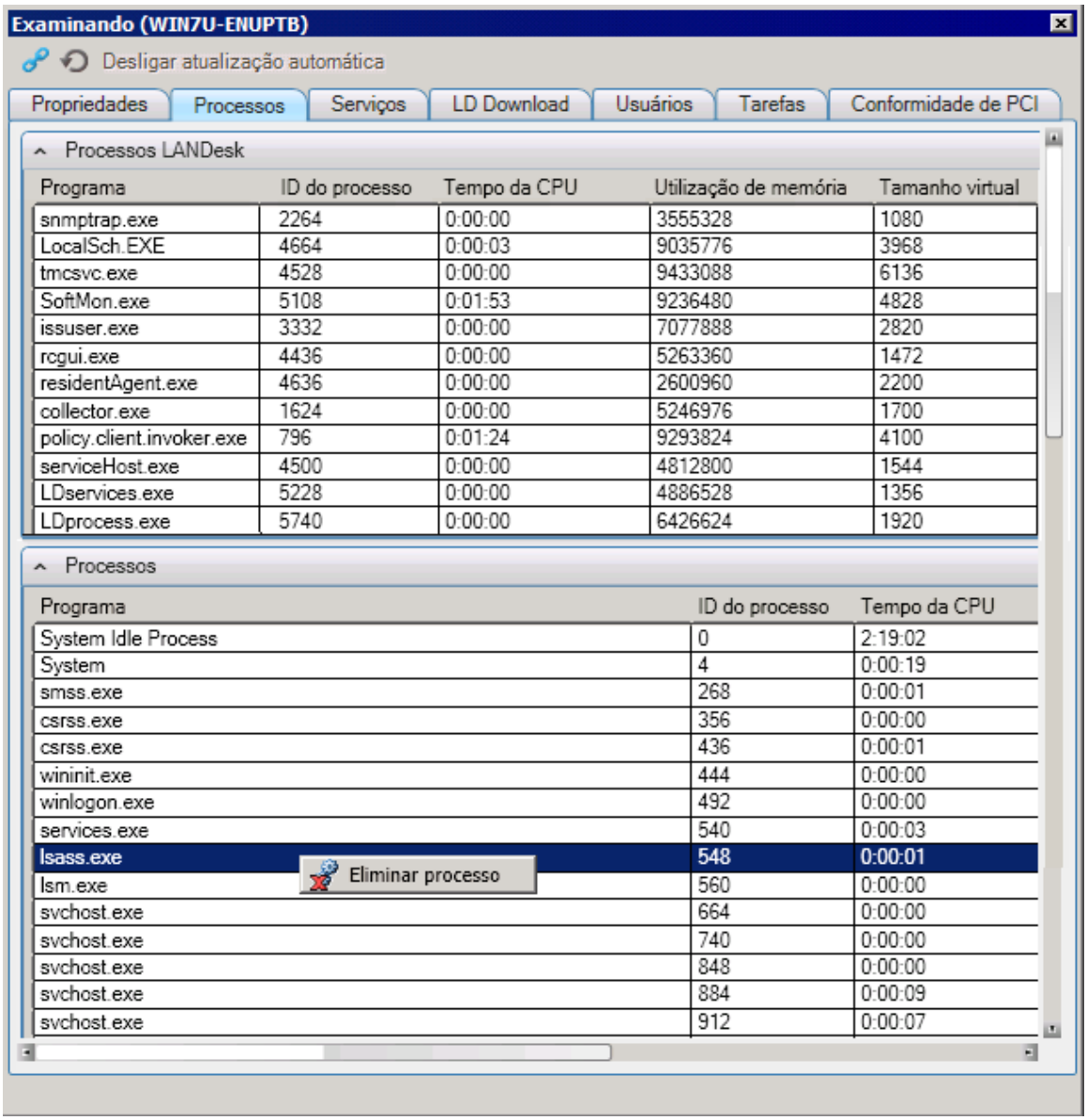


Visualização dos dados de inspetor

As janelas de inspetor contêm etiquetas diferentes e dados. Os itens são exibidos baseado no arquivo de XML definiu para esse item. Por exemplo, um inspetor padrão é fornecido para dispositivos administrados. Quando você clica um dispositivo administrado, você vê as seguintes etiquetas na janela de inspetor:



Você pode redimensionar a janela para exibir dados. Você pode agir em alguns itens, tal como a lista de processos em execução em execução em um dispositivo gerenciado. Da janela de inspetor, você pode clicar a **etiqueta** de Processos, direito-clique um processo na lista, e mata o processo.

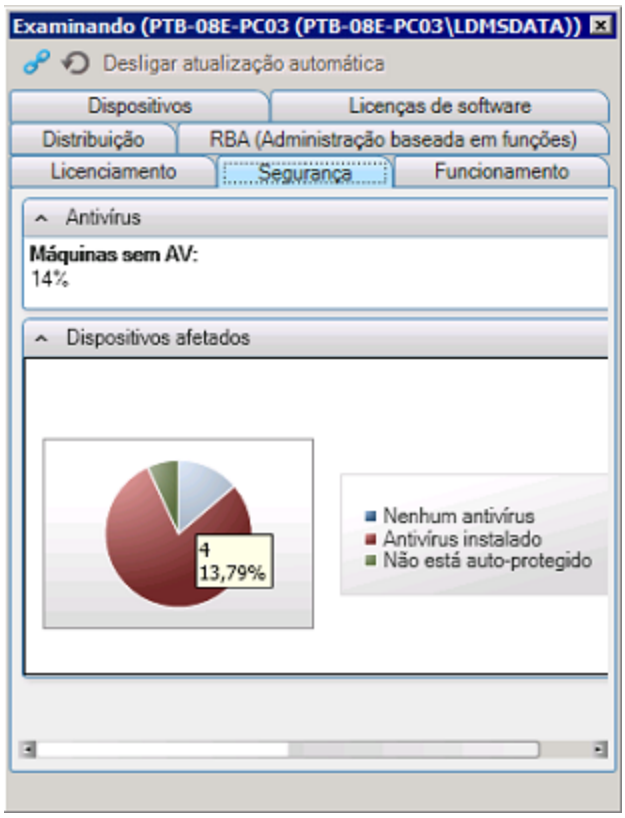


Da mesma forma, você pode parar ou iniciar serviços em execução em um dispositivo clicando na guia **Serviços** e clicando com o botão direito em um serviço na lista.

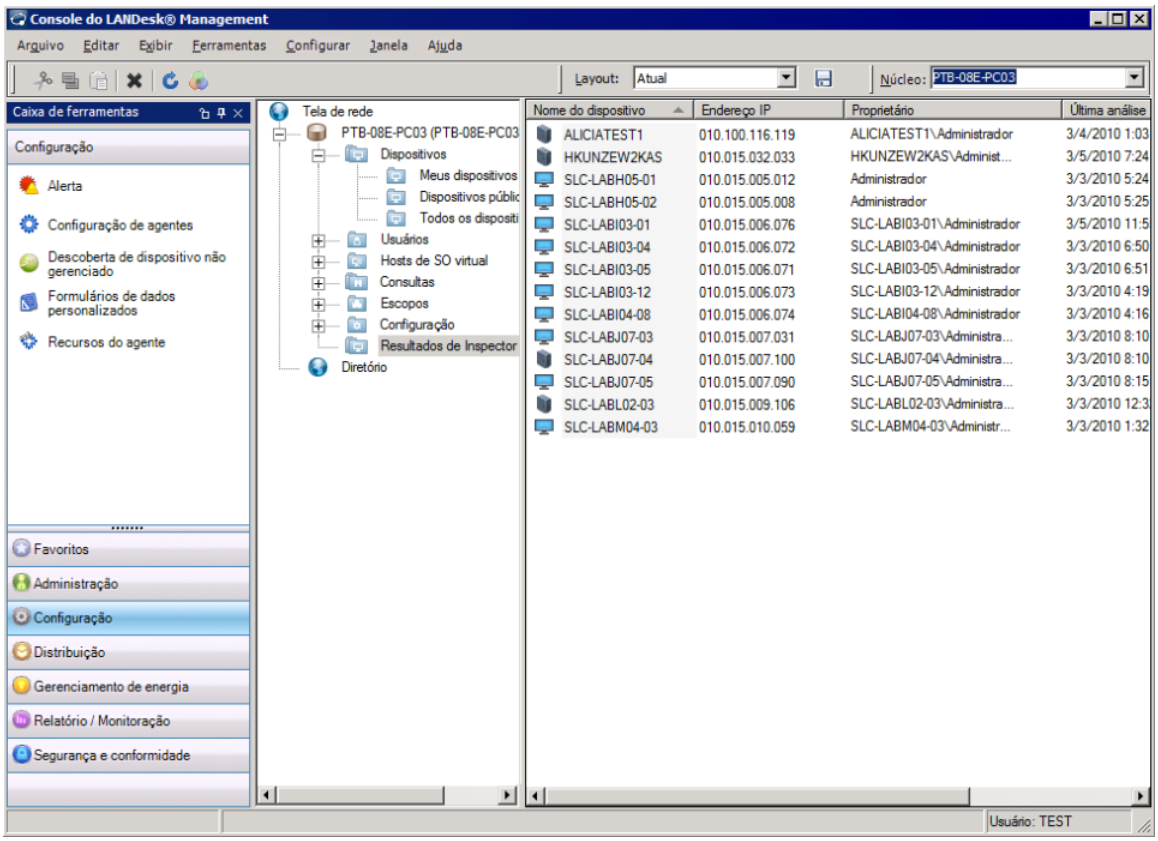
Visualização dos resultados do inspetor

Alguns itens de dados em uma janela de inspetor são exibidos como gráficos. Para exibir os detalhes de um mapa, duplo clique no mapa. Os detalhes de dados são exibidos na tela de rede nos **resultados de Inspetor** lista.

Cada mapa mostra um resumo de dados quando você aponta a uma porção do mapa.



Clique duas vezes o mapa para exibir os dados associados em formato de lista.



Ver os resultados que esta maneira faz os dados litigável. Por exemplo, no inspetor Programado de tarefas um mapa pode mostrar quantos dispositivos falhou uma tarefa. Se você clicar duas vezes o mapa, você verá os dispositivos individuais listados na pasta **de resultados de Inspetor** . Você então pode aplicar uma ação a esses dispositivos (tal como começar de na tarefa) ou vê um relatório com que dados acompanhar.

Os dados na pasta **de resultados de Inspetor** muda cada vez você clica duas vezes em um mapa em uma janela de inspetor. No exemplo acima, você clicaria no "Não anti-vírus" seção de um mapa ver uma lista de dispositivos sem uma aplicação de antivírus. Se você clica o "Anti-Vírus instalou" seção do mapa, a lista muda exibir dispositivos com uma aplicação de antivírus.

Dados de tempo real em inspetores

Alguns dados de inspetor podem ser atualizados em tempo real. Isto só pode acontecer se você dispôs um agente de dispositivo que inclui o estoque de tempo real e componente de monitoração.

Verificar se um dispositivo tem o estoque de tempo real e agente de monitoração

1. Na tela de rede, clique com o botão direito no dispositivo e selecione **Propriedades**.
2. Clique na guia **Agentes**.

Inspetores padrão

Os seguintes inspetores de predefined são incluídos quando você instala o add-on de inspetor:

- Configurações de coluna
- O computador inquire

- Usuários do console
- O usuário de console agrupa
- Servidores núcleo
- Métodos de entrega
- Pacotes de distribuição
- Consultas
- Funções
- Tarefas agendadas
- Escopos
- Scripts
- Equipes
- Vulnerabilidades

Criação de inspetores personalizados

Você pode criar um arquivo de XML que define parâmetros de inspetor para itens no Console de Gerência de LANDesk. Para fazer isto, você deverá conhecer convenções de XML e você deverá entender como dados é administrado na banco de dados seus usos de servidor núcleo.

Para instruções em criar um inspetor personalizado, consulte o " Criando um inspector" personalizado; documento na Comunidade de LANDesk.

NOTA: A ajuda do Inspetor na Comunidade de usuários da LANDesk
A comunidade de usuários da LANDesk tem documentos técnicos e fóruns de usuário para o inspetor. Para acessar a comunidade, vá a: http://community.landesk.com

Itens auto-inspecionados

Use the Auto-inspect feature to display detailed information about any item you click. Each time you click a new item, the contents of the inspector window change to show the new item.

1. Click **View > Auto Inspector**.
2. Click an item in a list, such as a managed device, a scheduled task, or a vulnerability.

Unlinking an auto-inspector window

If you want to keep the data in an auto-inspector window, unlink the inspector.

1. Clique em **Relatório**.

This keeps the current data in an inspector window, and you can then click other items that open in a new auto-inspector.

For example, you might unlink the data if you want to compare more than one item side by side. You would unlink the first data window and then click a new item to open a second inspector window.

Itens inspecionados manualmente

If you don't use Auto-inspect, you can inspect any item by right-clicking it. Each time you manually inspect an item, a new inspector window opens with the new data.

1. Right-click a list item (such as a managed device).
2. Select **Inspect**.

Desvinculando conteúdo dinâmico

Data in the inspector window can be dynamic. Some data items will refresh on a regular basis (if a device has the real-time inventory component).

To keep the data currently displayed in an inspector

1. Clique no botão **Desvincular** .

Refreshing data in an unlinked window

After you unlink an inspector window, you can't re-link the data to make the data dynamic again. The data in the window stays the same unless you change the refresh setting.

To refresh data in an inspector

1. Clique no botão **Alterar taxa de atualização**

.
2. The text next to the button indicates the current refresh setting. Click the button again to change the setting, which can be 10 seconds, 30 seconds, or 10 minutes.

Gerenciamento de usuários

Visão geral da administração com base em funções

LANDesk Management Suite permite gerenciar usuários de console com um conjunto extenso de recursos de administração baseada em função: É possível:

- Atribuir permissõe de grupo baseada em recurso granular
- Atribuir facilmente permissões para múiltiplos usuários através de grupos de usuários locais ou LDAP
- Sincronizar configurações de usuário de console entre múltiplos servidores núcleos

Você pode criar funções de acordo com as responsabilidades do usuário, com as tarefas administrativas que deseja que eles possam executar e com os dispositivos que deseja que eles possam ver, acessar e gerenciar. O acesso aos dispositivos pode ser restrito a uma localização geográfica, como um país, uma região, um Estado, uma cidade ou, até mesmo, um único escritório ou departamento. Ou, pode ser restrito a uma plataforma de dispositivo específica, a um tipo de processador ou a algum outro atributo de hardware ou software. A administração com base em funções, possibilita o controle total sobre o número de funções diferentes que você deseja criar, sobre que usuários poderão atuar nessas funções e sobre o escopo do acesso aos dispositivos. Por exemplo, você pode ter um ou mais usuários cuja função seja "gerente de distribuição de software", outro usuário responsável por operações de controle remoto, um usuário que executa relatórios, e assim por diante.

Se não tiver muitos usuários de console ou se não quiser limitar os usuários do console existentes, você pode ignorar completamente a administração baseada em função e apenas adicionar usuários ao grupo Administradores LANDesk do servidor núcleo. Os membros deste grupo tem acesso pleno ao console e pode gerenciar todos os dispositivos. Como padrão, a conta usada para instalar o Management Suite é colocada no grupo Administradores LANDesk.

A administração com base em funções é suficientemente flexível para permitir a criação de tantas funções personalizadas quanto necessárias. É possível atribuir as mesmas poucas permissões a diferentes usuários, mas restringir seu acesso a um conjunto limitado de dispositivos com um escopo reduzido. Até mesmo um administrador pode ter seu escopo limitado, tornando-o, essencialmente, um administrador de uma região geográfica específica ou de um tipo de dispositivo gerenciado. A forma como a administração com base em funções será aproveitada depende dos recursos de rede e pessoal, além das suas necessidades específicas.

NOTA: Se esta for uma atualização do Management Suite 8, a configuração cria um arquivo de registro chamado ...\LANDesk\Management Suite\RBAUpgradeReport.txt. Este arquivo tem informações para ajudá-lo a mapear funções 8.x para 9.x.

Para ver mais informações sobre o uso de funções, consulte as seções a seguir:

- "Adição de usuários do console do Management Suite" na página 39
- "Gerenciar autenticações" na página 42
- "Funções de gerenciamento" na página 43
- "Direitos e estados" na página 45
- "Criação de escopos" na página 54
- "Uso de equipes" na página 57

Fluxo de trabalho da Administração com base em funções

O seguinte é o processo básico para uso da administração baseada em função:

1. Criar funções para usuários do console.
2. Use a ferramenta Usuários e Grupos para adicionar usuários do console aos grupos apropriados do Windows LANDesk.
3. Criar autenticações para cada Diretório ativo (Active directory) que você estará usando para designar usuários de console.
4. Opcionalmente usar escopos para limitar a lista de dispositivos que usuários do console podem gerenciar.
5. Opcionalmente usar equipes para categorizar mais os usuários de console.

Adição de usuários do console do Management Suite

Os usuários do Management Suite podem fazer login no console e realizar determinadas tarefas em dispositivos específicos da rede. O usuário conectado ao servidor durante a instalação do Management Suite é inserido automaticamente no grupo de usuários do **LANDesk Management Suite** para Windows, que dá a eles permissões de administrador. Esse indivíduo é responsável pela adição de grupos ao console e pela atribuição de permissões e escopos. Quando outros administradores forem criados, eles poderão realizar as mesmas tarefas administrativas.

A configuração do Management Suite cria vários grupos locais do Windows no servidor núcleo. Esses grupos controlam as permissões de sistema de arquivo para as pastas de programa do Management Suite no servidor núcleo. Você precisa adicionar manualmente os usuários do console a um desses grupos locais do Windows:

- **LANDesk Management Suite:** Este grupo permite acesso básico ao núcleo. As pastas do Management Suite são somente para leitura. Os usuários neste grupo não podem gravar no diretório de scripts, portanto eles não podem gerenciar script. O patch de vulnerabilidades e a distribuição de SO não funcionarão corretamente neste grupo porque ambos usam scripts.
- **Gravadores de script LANDesk:** Este grupo permite que usuários gravem na pasta de scripts. Patch de vulnerabilidades e distribuição de SO precisam fazer parte deste grupo. Este grupo não concede qualquer outros privilégios administrativos.
- **Administradores LANDesk:** Este é um grupo à prova de falha para acesso ao console. Qualquer um nesse grupo tem direitos totais no console, inclusive o de gravar script. Como padrão, a conta de usuário que instalou o Management Suite é adicionada a este grupo. Se não tiver muitos usuários de console ou se não quiser limitar os usuários do console existentes, você pode ignorar completamente a administração baseada em função e apenas adicionar usuários a este grupo.

Ao adicionar administradores totais ao console, você pode adicioná-los ao grupo Administradores LANDesk do servidor núcleo local ou pode adicioná-los a um grupo diferente que tem o direito "Administrador" LANDesk . A única diferença é que os usuários no grupo Administradores LANDesk Windows não podem ser excluídos do console até serem removidos do grupo Administradores LANDesk.

A árvore **Usuários e grupos** da ferramenta de usuários exibe a lista com os usuários de console autorizados. É possível exibir o último acesso de um usuário de console, seu grupo, função, escopo, status de limite de tempo de controle remoto e a equipe. Você também pode usar esta árvore para verificar se os usuários estão nos grupos locais LANDesk do Windows. Os usuários não poderão fazer logon até que você os tenha adicionado-os à um dos grupos LANDesk descritos nesta seção.

Os usuários são armazenados no banco de dados por identificadores de segurança únicos (SIDs). Se um nome na conta de um usuário do active directory é alterado, por exemplo, se eles se casam o SID permanecerá o mesmo e suas permissões do Management Suite ainda serão válidas.

IMPORTANTE: Os consoles adicionais e o servidor núcleo precisam fazer parte do mesmo domínio ou workgroup (grupo de trabalho). Os usuários de console não conseguirão autenticar no servidor núcleo que estiver em um diferente domínio ou grupo de trabalho.

Adicionar usuários do console Management Suite

Os usuários do Management Suite podem fazer login no console e realizar determinadas tarefas em dispositivos específicos da rede. O usuário conectado ao servidor durante a instalação do Management Suite é inserido automaticamente no grupo de usuários do **LANDesk Management Suite** para Windows, que dá a eles permissões de administrador. Esse indivíduo é responsável pela adição de grupos ao console e pela atribuição de permissões e escopos. Quando outros administradores forem criados, eles poderão realizar as mesmas tarefas administrativas.

Para adicionar usuários ao grupo um LANDesk da caixa de diálogo Gerenciamento de computador do Windows

1. Navegue até o utilitário do servidor **Ferramentas administrativas > Gerenciamento de computadores > Usuários e Grupos locais > Grupos**.
2. Clique com o botão direito no grupo LANDesk que desejar e, em seguida, clique em **Adiciona grupo**.
3. Na caixa de diálogo **Propriedades**, clique em **Adicionar**.
4. Na caixa de diálogo **Selecionar usuários e grupos**, selecione os usuários (e grupos) desejados da lista e clique em **Adicionar**.
5. Clique em **OK**.

Para adicionar um usuário ou grupo do console do Management Suite

1. Clique em **Ferramentas > Administração > Gerenciamento de usuários**.
2. Na árvore **Usuários e grupos**, clique com o botão direito na origem da autenticação contendo o usuário ou grupo desejado e clique em **Novo usuário ou grupo**
3. No diretório de origem da autenticação, selecione o usuário ou o grupo que você deseja adicionar e clique em **Adicionar**. Se você quiser selecionar usuários individuais dentro de um grupo, clique com o botão direito no grupo e clique em **Selecionar usuários para adicionar**. Em seguida, você pode selecionar os usuários que você deseja e clique em **Adicionar usuários selecionados**.
4. Na caixa de diálogo lembrando-o de adicionar manualmente o usuário ou grupo selecionado ao grupo local LANDesk do Windows apropriado, clique em **OK**.
5. Clique em **Fechar**.
6. Use a ferramenta **Usuários e grupos locais** do Windows para adicionar o novo usuário ou grupo ao grupo apropriados do Windows LANDesk conforme descrito anteriormente nesta seção.
7. Atribua funções e escopos ao novo usuário ou grupo.

Excluir usuários

Você também pode usar a árvore **Usuários e grupos** para excluir usuários e ou grupos de console. Quando exclui um usuário ou grupo, você é solicitado a decidir o modo como deseja lidar com os itens do console que pertencem a eles, por exemplo, consultas, tarefas agendadas, etc. Você pode fazer o console excluir automaticamente qualquer item pertencente aos usuário ou pode fazer o console atribuir novamente esses itens a outros usuários ou grupos que selecionar. Observe que a exclusão de um usuário ou grupo só exclui este usuário ou grupo do banco de dados do usuário do Management Suite. Você necessitará também excluir o usuário ou grupo manualmente dos grupos locais LANDesk do Windows dos quais eles são membros. Se não fizer isso, o usuário excluído ainda poderá fazer login no console.

Para excluir um usuário do console

1. Clique em **Ferramentas > Administração > Gerenciamento de usuários**.
2. Na árvore **Gerenciamento de usuários**, clique em **Usuários e grupos.**
3. Selecione o usuário ou grupo que você quer excluir e pressione a tecla Delete.
4. Se você quiser excluir objetos associados ao usuário, clique em **OK**.
5. Se você quiser atribuir objetos associados novamente ao usuário do console, selecione **Atribuir objetos ao seguinte usuário/grupo ou equipe** e clique no usuário, grupo ou equipe que você deseja que receba os objetos e clique em **OK**.
6. Remova o usuário do grupo local LANDesk do Windows ou grupo do Active Directory que dá acesso ao console.

Exibição das propriedades do usuário ou grupo

Na árvore **Usuários e grupos**, você pode clicar com o botão direito em um usuário ou grupo no painel da direita e clique em **Propriedades**. Esta caixa de diálogo de propriedades exibe todas as propriedades e permissões válidas este usuário. A caixa de diálogo Propriedades contém as seguintes páginas:

- **Resumo:** Resume as funções do usuário/grupo escopos, equipes, participação em grupos e permissões válidas.
- **Permissões válidas:** Apresenta uma exibição mais detalhada das permissões válidas do usuário/grupo.
- **Funções:** Exibe as funções herdadas e explícitas. Você pode selecionar quais funções explícitas se aplicam a esse usuário ou grupo.
- **Escopos:** Exibe os escopos herdados e explícitos. Você pode selecionar quais escopos explícitos se aplicam a esse usuário ou grupo.
- **Equipes:** Exibe as equipes herdadas e explícitas. Você pode selecionar quais equipes explícitas se aplicam a esse usuário ou grupo.
- **Limites de tempo do controle remoto:** Permite que você aplique e modifique os limites de tempo do controle remoto. Para obter mais informações, consulte "Uso de restrições de tempo do controle remoto" na página 57.
- **Membro de grupo:** Exibe os grupos dos quais o usuário é membro.
- **Membros do grupo:** Exibe os membros de um grupo se um grupo estiver selecionado. Exibe o grupo do qual um usuário é membro se o usuário estiver selecionado.

Se você fizer alterações nas páginas editáveis, você precisa clicar em OK para aplicá-las. Em seguida, é possível reabrir a caixa de diálogo propriedades, se for necessário.

Gerenciar autenticações

Use a ferramenta Gerenciamento de usuários para definir credenciais para os grupos Active Directory que terão acesso ao console. Essas credenciais só precisam deixar o Management Suite enumerar o diretório. Você precisará fornecer credenciais para cada Active Directory que contém usuários aos quais deseja dar acesso ao console. As autenticações que fornecer determinarão de que grupos de usuários você pode selecionar usuários para atribuir permissões de grop a console.

A autenticação de console é baseada no grupo local Windows ou Active Directory. Quando um administrador LANDesk atribui permissões de grupo a um grupo local ou Active Directory, os usuários membros desse grupo podem acessar os consoles Windows ou da Web e compartilhar as permissões atribuídas àquele grupo.

É necessário estar ciente dos seguintes problemas ao gerenciar Active Directories (diretórios ativos) para uso com o Management Suite:

- O Active Directory é totalmente integrado com o DNS e o TCP/IP (DNS) é necessário. Para ser totalmente funcional, o servidor DNS deve ser compatível com registros de recurso SRV ou registros de serviço)
- O uso do Active Directory para adicionar um usuário ao grupo sendo utilizado no console não habilita o usuário a acessar o console mesmo se o usuário tiver permissões Management Suite a ele atribuídos. Para acessar o console, o usuário precisa pertencer aos grupos LANDesk local do servidor núcleo. Para obter mais informações, consulte "Adição de usuários do console do Management Suite" na página 39.
- Para os Active Directories funcionarem corretamente com a administração baseada em funções, é necessário configurar as credenciais de servidor COM+ no servidor núcleo. Isso habilita o servidor núcleo a usar uma conta em um dos grupos LANDesk local do servidor núcleo que tem as permissões necessárias para enumerar os membros do domínio Windows, como a conta de administrador. Para ver as instruções sobre como fazer a configuração, consulte "Configuração das credenciais do servidor COM+" na página 74.

Se a senha da conta para uma autenticação mudar você precisará entrar no console e mudar a senha na caixa de diálogo para aquela nova senha. Você pode fazer isso acessando como um grupo local. Os usuários são autenticados quando acessam, portanto as sessões existentes continuarão a funcionar. Os usuários no domínio que tiverem a senha trocada não terão permissão de acesso até que a senha mude da forma como foi corrigida na ferramenta Usuários.

Definir direitos com o Active Directory

As seguintes regras se aplicam quando usar o Active Directory com RBA:

- Se um usuário for membro de um grupo do Active Directory, o usuário herda as permissões RBA para aquele grupo.
- Se um usuário for membro de um grupo Active Directory, que é membro de um grupo de nível mais alto, o usuário herda os direitos RBA do grupo de nível superior.
- Grupos podem ser aninhados e herdar os direitos adequados de acordo com as regras normais do Active Directory.

Adicionar uma autenticação do Active directory

Use a ferramenta Gerenciamento de usuários para definir credenciais para os grupos Active Directory que terão acesso ao console. Essas credenciais só precisam deixar o Management Suite enumerar o diretório. Você precisará fornecer credenciais para cada Active Directory que contém usuários aos quais deseja dar acesso ao console. As autenticações que fornecer determinarão de que grupos de usuários você pode selecionar usuários ao atribuir permissões de grupo a console.

Para adicionar uma autenticação

1. Na ferramenta **Gerenciamento de usuário**, clique com o botão direito em **Usuários e grupos** e em **Nova origem de autenticação**.
2. Na caixa de diálogo **Autenticação de origem**, digite as credenciais que dão acesso ao Active Directory.
3. Clique em **OK**.

Ajuste da frequência de pesquisa do diretório

A partir do LDMS 9, SP2, existe um utilitário chamado Resolveusergroups.exe. Esse utilitário é executado periodicamente (a cada 20 minutos) para atualizar a lista de usuários do LANDesk Management Suite.

Uma vez que a lista de usuários estiver resolvida, ela é colocada em cache e usada até que o Resolveusergroups.exe seja executado novamente. Em alguns ambientes do Active Directory, se os valores de TTL forem pequenos demais, algumas contas de usuários resolvidas podem ter ultrapassado o limite de TTL antes que todas as contas sejam resolvidos. Isso faz com que o cachê seja refrescado repetidas vezes e as cargas do console sejam muito lentas.

Se isso acontecer no seu ambiente, mude as configurações padrão do TTL pra Resolveusergroups.exe. Você pode executar o Resolveusergroups.exe /? para visualizar o uso. Os valores TTL são exibidos em segundos. Um exemplo específico de configuração de valores máximos de TTL:

```
Resolveusergroups.exe /verbose /TTL 600 /LDTTL 60
```

Todas as mudanças nos valoresTTL são escritas em na tabela KeyValue do banco de dados (GroupResolutionTTL e LocalLDGroupResolutionTTL), para que sejam persistentes.

Funções de gerenciamento

Use a árvore de Funções para definir e manter funções administrativas e seus direitos de console associados. Direitos de console são baseados nos recursos do Management Suite. Por exemplo, você pode criar uma função de ajuda e dar a ela o direito de controle remoto.

Você pode adicionar quantas funções precisar. Novas funções não são automaticamente atribuídas a nenhum usuários ou grupos. Ao criar uma função, você associa-a a um usuário ou grupo na árvore Permissões de grupo.

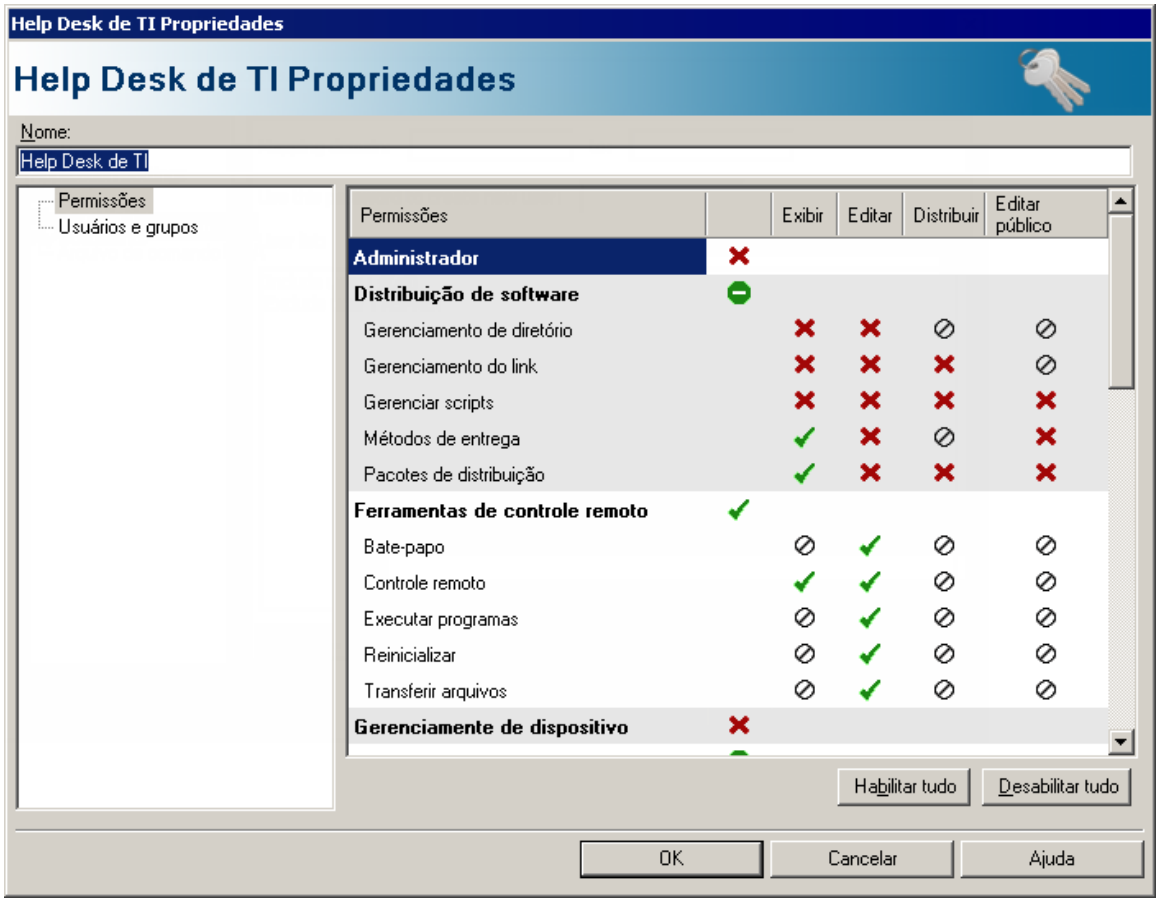
Como você pode atribuir múltiplas funções à usuários ou grupos, decida como quer atribuir direitos. Você pode atribuir direitos baseados em uma descrição de tarefa como "help desk" ou pode atribuir direitos baseados em recursos de console como "controle remoto." Dependendo do número e da variedade de usuários de console que a sua organização tiver um modo pode funcionar melhor que outro.

Você pode atribuir múltiplas funções a um usuários ou grupo do Active Directory. Se houver permissões em conflito entre as funções selecionadas, a permissão de grupo consiste na soma das funções e escopos combinadas. Por exemplo, se uma função inclusa permitir controle remoto e outra função inclusa a negar, a permissão de grupo resultante permitirá o controle remoto. Você pode exibir as permissões válidas de um usuário ou grupo ao abrir as propriedades e abrir a página **Permissões válidas**.

Em geral, você deve evitar atribuir funções à grupos locais padrão: LANDesk Management Suite, Gravadores de script LANDesk e Administradores LANDesk. Atribuir uma função à um grupo a um grupo afeta todos dentro do grupo. Como todos os usuários de console precisam ser membros de um desses três grupos, você poderia inadvertidamente restringir o acesso de todos aos recursos do console. O grupo Administradores da LANDesk já tem uma função padrão de Administrador, que você não pode restringir no futuro.

Mudanças nas permissões de usuários conectados não terão efeito até o próximo logon.

Para obter mais informações, veja "Direitos e estados" na página 45 e "Funções padrão" na página 45.



Criar e atribuir uma função

Use Funções para definir e manter funções administrativas e seus direitos de console associados.

Criar e atribuir uma função

1. Na ferramenta **Gerenciamento de usuário**, clique com o botão direito em **Funções** e em **Nova função**.

2. Na caixa de diálogo **Propriedades da função**, digite um **Nome da função**
3. Habilite ou desabilite os direitos que deseja, clicando no símbolo na coluna adequada. Cada clique alterna o estado do direito.
4. Na árvore, clique em **Usuários e grupos** e selecione os usuários e grupos que terão uma nova função.

Para atribuir uma função à usuários e grupos existentes

1. Na ferramenta **Gerenciamento de usuário**, clique com o botão direito em **Funções** e em **Propriedades**. Você também pode clicar duas vezes em uma regra para editar suas propriedades.
2. Na página **Usuários e grupos**, selecione os grupos que terao aquela função.
3. Clique em **OK**.

Funções padrão

Existe um número de funções padrão na árvore de Funções. É possível excluir ou editar qualquer uma dessas funções padrão, exceto a do Administrador LANDesk.

- Configuração da auditoria
- Auditor
- Visualizador do inspetor
- Help Desk de TI
- Administrador LANDesk
- Gerenciamento de patches
- Gerenciamento de energia
- Provisionamento
- Segurança
- Distribuição de software
- Licenciamento de software

IMPORTANTE: Administradores da LANDesk têm permissões totais
Administradores da LANDesk tem direitos plenos a todos os escopos e direitos. Eles têm também acesso total à ferramenta Usuários e pode fazer qualquer mudança que quiser. Além disso, somente usuários com o direito de Administrador podem configurar serviços da LANDesk em execução no núcleo.

Direitos e estados

Há quatro tipos de direitos que um usuário pode ter:

- **Exibir:** Permite usuários acessar uma ferramenta de console.
- **Editar:** Permite aos usuários fazerem mudanças na ferramenta associada de console. Inclui o direito de ver.
- **Distribuir:** Permite aos usuários criarem, modificarem ou excluirem qualquer tarefa agendada associada à ferramenta associada de console.
- **Editar público:** Permite aos usuários criarem, modificarem ou excluirem itens em uma pasta **Pública** da ferramenta de console.

Nem todos os direitos suportam todos os tipos. Por exemplo, o direito "Gerenciamento de consulta pública" só pode ter o tipo "Editar público". Não teria sentido que ele tivesse também os tipos "Ver", "Editar" ou "Distribuir".

Um direito pode ter três estados:

- Uma marca de seleção: ✔
- Um X: ✖
- Um símbolo não aplicável: ⊘

Clique em uma marca de verificação ou em um X para alternar entre estados.

Se os usuário não tiverem direitos a uma ferramenta, eles não verão a ferramenta quando acessarem o console. A ferramenta não aparecerá na Caixa de ferramentas ou no menu **Ferramentas**.

A ferramenta **Tarefas agendadas** só é visível para usuários que têm um direito "Distribuir" e nesse caso, eles só podem trabalhar com tarefas associadas com a ferramenta para a qual eles têm direitos de distribuir. Todas as outras tarefas são somente para leitura.

Direito "Editar público"

Um grupo Público da ferramenta é visível a todos os usuários. Itens no grupo público são somente leitura, a menos que você tenha o direito "Editar público". Os usuários que têm direitos "Editar público" para um recurso podem somente editar itens públicos para aquele recurso. Outros itens públicos são somente leitura. Itens de somente leitura ainda são úteis, pois os usuários podem copiar esses itens para o grupo da árvore "Meu ..." e editá-los ali.

O grupo Público da ferramenta **Tarefas agendadas** funciona ligeiramente diferente. Todas as tarefas no grupo Público são visíveis aos usuários com um direito de "distribuir", inclusive tarefas para recursos para os quais os usuários podem não ter acesso. Entretanto, somente as tarefas para as quais os usuários têm um direito de "Distribuir" são editáveis. O resto é somente para leitura.

Se você tiver tipos de direito "Editar Público" e "Distribuir", você pode criar novas tarefas no grupo Público e adicionar/remover tarefas dele.

Referência a direitos de console

Os direitos de console dão acesso a ferramentas Management Suite e recursos específicos. Os usuários devem ter os direitos necessários para realizar tarefas correspondentes. Por exemplo, para controlar dispositivos remotamente no seu escopo, o usuário precisa fazer parte de um grupo que tem direito de controle remoto.

A administração baseadas em funções envolve as seguintes permissões:

- Administrador
- Configuração de agentes
- Alertas
- Web console básico
- Replicação de conteúdo
- Sincronização do núcleo
- Formulários de dados personalizados
- Gerenciamento de dispositivo

    - Adicionar ou excluir dispositivos
    - Monitoração de dispositivos
    - Controle de energia do dispositivo
    - Gerenciar usuários e grupos locais
    - Gerenciar grupos públicos de dispositivo
    - Descoberta de dispositivos não gerenciados
- Inspetor
- Gerenciamento de link
- Distribuição-provisionamento de OS
- Gerenciamento de energia
- Gerenciamento de consultas públicas
- Atualizar escopos
- Ferramentas de controle remoto
    - Bate-papo
    - Executar programas
    - Reinicializar
    - Controle remoto
    - Transferir arquivos
- Relatórios
    - Designer de relatório
    - Relatórios
- Segurança
    - Controle de acesso à rede
    - Patch e conformidade
    - Configurações de segurança
- Distribuição de software
    - Métodos de entrega
    - Gerenciador de diretório
    - Pacotes de distribuição
    - Gerenciamento de link
    - Gerenciar scripts
- Monitoração de licenças de software
- Administração de usuário
- vPro

Veja as descrições abaixo para saber mais sobre cada permissão e sobre como elas podem ser usadas para criar funções administrativas.

NOTA: O escopo controla o acesso aos dispositivos
Ao utilizar os recursos permitidos por essas permissões, os usuários sempre estarão limitados pelo seu escopo (os dispositivos que poderão ver e manipular).

Administrador Management Suite

A permissão de Administrador Management Suite oferece acesso total a todas as ferramentas do aplicativo (entretanto, o uso dessas ferramentas ainda está limitado aos dispositivos incluídos no escopo do administrador).

A permissão de Administrador Management Suite dá aos usuários a habilidade de:

- Gerenciar usuários com a ferramenta Usuários.
- Ver e configurar o licenciamento de produtos no menu **Configurar**.
- Configurar serviços LANDesk.
- **IMPORTANTE:** Execute TODAS as tarefas do Management Suite permitidas pelas outras permissões

Configuração de agentes

- Sem permissões: Não pode ver a ferramenta.
- Exibir: Pode ver esta ferramenta e pode ver qualquer coisa. Não pode mudar nada.
- Editar: Pode ver e mudar qualquer coisa. Não pode distribuir uma tarefa de configuração do agente.
- Distribuir: Pode ver tudo. Não pode mudar nada. Pode agendar qualquer tarefa de configuração de agente que puder ver (inclusive pública).
- Editar público: Pode atribuir configuração ao público. Pode editar configurações públicas.

Alertas

- Sem permissões: Não pode ver a ferramenta.
- Exibir: Pode ver esta ferramenta e pode ver qualquer coisa. Não pode mudar nada.
- Editar: Pode ver e mudar qualquer coisa. Não pode distribuir.
- Distribuir: Pode ver tudo. Não pode mudar nada. Pode distribuir.

Web console básico

- Sem permissões: Não pode acessar o Web console.
- Exibir: Não aplicável.
- Editar: Pode acessar o Web console e ver aspectos mais básicos.
- Distribuir: Não aplicável.

Replicação de conteúdo

- Sem permissões: Não pode ver a ferramenta.
- Exibir: Pode ver esta ferramenta e pode ver qualquer coisa. Não pode mudar nada.
- Editar: Pode ver e mudar qualquer coisa.
- Distribuir: Não aplicável.

Sincronização do núcleo

- Sem permissões: Sem ferramenta de sincronização do núcleo. Sem opções de clique do botão direito para **Autosincronizar** ou **Copiar para núcleo**. Ainda mostra opções de importação e exportação. (Elas são associadas ao direito "Editar" para a ferramenta que tem essas opções.)
- Exibir: Pode ver a ferramenta, mas não pode fazer nenhuma mudança. Ainda sem opções de sincronização nos menus de contexto conforme mostrado acima.

- Editar: Pode fazer tudo. Adicionar/remover núcleos alvo, ligar e desligar componentes, habilitar sincronização automática em instâncias e sincronização manual.
- Distribuir: Não aplicável.

Formulários de dados personalizados

- Sem permissões: Não pode ver a ferramenta.
- Exibir: Pode ver esta ferramenta e pode ver qualquer coisa. Não pode mudar nada.
- Editar: Pode ver e mudar qualquer coisa. Não pode distribuir.
- Distribuir: Pode ver tudo. Não pode mudar nada. Pode distribuir.

Gerenciamento de dispositivo

Adicionar/remover dispositivos

- Sem permissões:
  - Não pode ver a opção **Inserir novo computador** no menu de contexto quando abrir **Todos os dispositivos** na **Tela da rede**.
  - Não pode ver a opção **Excluir** no menu de contexto quando selecionar um dispositivo na **Tela da rede**.
  - Não pode ver o nó da árvore **Tela da rede > Configuração > Computadores adicionados pelo usuário**.
- Exibir: Não aplicável.
- Editar:
  - Pode ver e usar a opção **Inserir novo computador** no menu de contexto quando abrir **Todos os dispositivos** na **Tela de rede**.
  - Pode ver a opção **Excluir** no menu de contexto quando selecionar um dispositivo na **Tela a rede**.
  - Pode ver o nó da árvore **Tela da rede > Configuração > Computadores adicionados pelo usuário**.
- Distribuir: Não aplicável.

Monitoração de dispositivos

- Sem permissões: Não pode ver o **Monitoramento de dispositivo** do menu **Configurar**.
- Exibir: Pode ver a ferramenta Alertas e a ferramenta Logs. Pode ver informações na ferramenta de Monitoramento de dispositivo. Não pode editar.
- Editar: Pode ver a ferramenta Alertas e a ferramenta Logs. Pode ver e editar informações na ferramenta de Monitoramento de dispositivo.
- Distribuir: Não aplicável.

Controle de energia do dispositivo

- Editar: Pode ver e usar as opções **Ativar**, **Reinicializar** e **Desligar** no menu de contexto quando selecionar um dispositivo.

Gerenciar usuários e grupos locais

- Editar: Pode ver e usar **Gerenciar usuários e grupos locais** no menu de contexto quando selecionar um dispositivo.

Gerenciar grupos públicos de dispositivo

- Sem permissões: Não pode mudar nada em **Dispositivos públicos**.
- Exibir: Não aplicável.
- Editar: Não aplicável.
- Distribuir: Não aplicável.
- Editar Público Pode criar, excluir e mudar grupos de dispositivos em **Dispositivos públicos**. Pode mudar um grupo de dispositivos para **Dispositivos públicos**.

Descoberta de dispositivos não gerenciados

- Sem permissões: Não pode ver a ferramenta UDD.
- Exibir: Pode abrir a ferramenta UDD e ver qualquer item. Não pode criar/excluir/editar nada.
- Editar: Pode abrir a ferramenta UDD e ver qualquer item. Pode criar/excluir/editar nada.
- Distribuir: Pode abrir a ferramenta UDD e ver qualquer item. Não pode criar/excluir/editar nada. Pode agendar uma tarefa UDD.

Inspetor

- Sem permissões: Não é possível ver a ferramenta de Inspeção.
- Exibir: Pode abrir a ferramenta de Inspeção e ver qualquer item.

Distribuição/provisionamento de SO

- Sem permissões: Não pode ver a ferramenta de Distribuição de SO.
- Exibir: Pode ver a ferramenta. Não pode mudar nada.
- Editar: Pode criar, editar e excluir itens. Não pode agendar uma tarefa.
- Distribuir: Pode agendar tarefas para itens que pode ver (inclusive públicas). Não pode criar, editar e excluir itens.
- Editar Público Pode mudar itens para a pasta Pública. Pode criar, editar ou apagar itens na pasta Pública.

Gerenciamento de energia

- Sem permissões: Não pode ver a ferramenta Gerenciamento de energia.
- Exibir: Pode ver a ferramenta. Não pode mudar nada.
- Editar: Pode criar, editar e excluir itens. Não pode agendar uma tarefa.
- Distribuir: Pode agendar tarefas para itens que pode ver (inclusive públicas). Não pode criar, editar e excluir itens.
- Editar Público Pode mudar itens para a pasta Pública. Pode criar, editar ou apagar itens na pasta Pública.

Gerenciamento de consultas públicas

- Sem permissões: Comportamento regular.
- Exibir: Não aplicável.
- Editar: Não aplicável.
- Distribuir: Não aplicável.
- Editar Público Pode mudar consultas para a pasta Pública. Pode criar, editar ou apagar consultas na pasta Pública.

Atualizar escopos

- Sem permissões: O botão barra de ferramentas **Atualizar escopos** da **Tela da rede** não faz nada.
- Editar: O botão barra de ferramentas **Atualizar escopos** da **Tela da rede** atualiza todos os escopos. Use isto quando tiver adicionado dispositivos a um escopo ou mudado um escopo de usuário e quiser que o usuário veja o novo escopo. Do contrário a atualização do escopo pode aguardar até uma hora antes de ocorrer automaticamente.

Ferramentas de controle remoto

Bate-papo

- Editar: Pode ver a opção **Controle remoto > Bate papo** e pode usá-lo. A opção **Bate papo** é habilitada na janela do Controle remoto.

Executar programas

- Editar: Pode ver a opção **Controle remoto > Executar programa** e pode usá-lo. A opção **Executar programa** é habilitada na janela do Controle remoto.

Reinicializar

- Editar: Pode ver a opção **Controle remoto > Reinicialização** e pode usá-la. A opção **Reinicialização** é habilitada na janela do Controle remoto.

Controle remoto

- Sem permissões: Não pode ver a opção **Controle remoto > Controle remoto** no menu de contexto.
- Exibir: Pode ver a opção **Controle remoto > Controle remoto** e pode controlar remotamente um dispositivo. Não pode assumir o controle do dispositivo (somente exibição).
- Editar: Pode ver a opção **Controle remoto > Controle remoto** e pode controlar remotamente e assumir controle de um dispositivo.
- Distribuir: Não aplicável.

Transferir arquivos

- Editar: Pode ver a opção **Controle remoto > Transferir arquivos** e pode usá-lo. A opção **Transferir arquivos** é habilitada na janela do Controle remoto.

Relatórios

Designer de relatório

- Sem permissões: Não pode abrir o designer.
- Exibir: Não aplicável.
- Editar: Pode abrir o designer e criar ou editar relatórios.
- Distribuir: Não aplicável.
- Editar público: Não aplicável.

Relatórios

- Sem permissões: Não pode visualizar a ferramenta.
- Exibir: Pode visualizar esta ferramenta e relatórios. Pode executar relatórios. Não pode alterar nada.
- Editar: Pode visualizar e alterar as propriedades do relatório. Esta permissão não dá acesso ao designer. A permissão editar é necessária para acessar o Report designer.
- Distribuir: Pode programar e poder publicar relatórios.
- Editar público: Pode mover relatórios para a pasta Pública.

Segurança

Controle de acesso à rede

- Sem permissões: Não pode ver a ferramenta.
- Exibir: Pode ver esta ferramenta e pode ver qualquer coisa (como configuração 802.1x). Não pode mudar nada.
- Editar: Pode ver e mudar qualquer coisa, inclusive publicar configurações NAC.
- Distribuir: Não aplicável.

Patch e conformidade

- Sem permissões: Não pode ver a ferramenta. Não pode ver nenhuma tarefa agendada ou diretivas na distribuição de software que são criadas com a ferramenta.
- Exibir: Pode ver a ferramenta. Pode ver tudo dentro. Não pode descarregar conteúdo, criar/editar/excluir configurações ou mudar nada. Acesso somente leitura.
- Editar: Pode ver a ferramenta. Pode ver tudo dentro. Pode editar qualquer coisa. Não pode agendar nada, incluindo: download de conteúdo, tarefas de análise, tarefas de reparo, levantamento de histórico etc.
- Distribuir: Pode ver a ferramenta. Pode ver tudo dentro. Não pode modificar nada, mas pode criar uma tarefa ou diretiva usando as informações ali encontradas para itens que pode ver (inclusive público).
- Editar Público Pode mudar itens para a pasta Pública. Pode criar, editar ou apagar itens na pasta Pública.

Configurações de segurança

- Sem permissões: Não pode ver a ferramenta. Não pode ver nenhuma tarefa agendada ou diretivas na janela Tarefas agendadas que são criadas com essa ferramenta.
- Exibir: Pode ver esta ferramenta e a ferramenta Atividade de segurança. Pode ver, mas não muda nenhuma configuração ou cria nenhuma tarefa.
- Editar: Pode ver a ferramenta e a ferramenta Atividades de segurança. Pode ver tudo dentro. Pode editar qualquer coisa. Não pode agendar nada.
- Distribuir: Pode ver a ferramenta e a ferramenta Atividades de segurança. Pode ver tudo dentro. Não pode modificar nada, mas pode criar uma tarefa ou diretiva para distribuir isso para um cliente ou mudar sua configuração para itens que pode ver (inclusive público).
- Editar Público Pode mudar itens para a pasta Pública. Pode criar, editar ou apagar itens na pasta Pública.

Distribuição de software

Métodos de entrega

- Exibir: Pode ver a ferramenta e tudo que há nela.
- Editar: Pode criar/editar/excluir métodos.
- Distribuir: Não aplicável.
- Editar Público Pode mudar itens para a pasta Pública. Pode criar, editar ou apagar itens na pasta Pública.

Gerenciador de diretório

- Exibir: Pode ver a ferramenta e tudo que há nela (assumindo-se que alguém já se autenticou).
- Editar: Pode autenticar em um novo diretório, pode ver tudo e pode criar/editar/excluir consultas.

- Distribuir: Não aplicável.

Pacotes de distribuição

- Exibir: Pode ver a ferramenta e tudo que há nela.
- Editar: Pode criar/editar/excluir pacotes.
- Distribuir:
  - Pode distribuir um pacote na ferramenta de pacote de distribuição.
  - Pode usar o botão **Criar tarefa de distribuição de software** na ferramenta Tarefas agendadas.
  - Pode usar o botão **Criar tarefa de script personalizado** na ferramenta Tarefas agendadas.
  - Isto se aplica a todos os itens que ele pode ver (inclusive públicas).
- Editar Público Pode mudar itens para a pasta Pública. Pode criar, editar ou apagar itens na pasta Pública.

Gerenciamento de link

- Sem permissões: Não pode ver a ferramenta Gerenciamento de link.
- Exibir: Pode ver a ferramenta. Não pode mudar nada.
- Editar: Pode criar, editar e excluir itens. Não pode agendar uma tarefa/diretiva.
- Distribuir: Não pode criar, editar e excluir itens. Pode agendar uma tarefa/diretiva.

Gerenciar scripts

- Exibir: Pode ver esta ferramenta e pode ver qualquer coisa. Não pode mudar nada.
- Editar: Pode ver e mudar qualquer coisa. Não pode agendar uma tarefa.
- Distribuir: Pode agendar tarefas para itens que pode ver (inclusive Públicas). Não pode criar, editar e excluir itens.
- Editar Público Pode mudar itens para a pasta Pública. Pode criar, editar ou apagar itens na pasta Pública.

Monitoração de licenças de software

- Sem permissões: Não pode ver a ferramenta de monitoramento de licença de software.
- Exibir: Pode ver tudo. Não pode mudar nada.
- Editar: Pode ver e editar qualquer coisa.
- Distribuir: Não aplicável.

Administração de usuário

- Sem permissões: Não pode ver a ferramenta Usuários.
- Exibir: Pode ver tudo. Não pode mudar nada.
- Editar: Não aplicável.
- Distribuir: Não aplicável.

vPro

- Sem permissões: Não pode ver nem mudar as informações e configurações do vPro.
- Exibir: Não aplicável.
- Editar: Pode ver e mudar informações e configurações do vPro.
- Distribuir: Não aplicável.

Informações adicionais sobre tarefas agendadas

- Se um usuário tem permissões de "Distribuição" para qualquer das ferramentas abaixo, ele pode ver a ferramenta de tarefa agendada.
- Se o usuário tem direitos de "Distribuição" ele pode ter direitos para modificar qualquer parte do tipo de tarefa para as quais ele tiver direito de "Distribuição" (por exemplo, configuração de agente, distribuição de software, Patch, etc.).
- Se o usuário tem direitos de "Distribuição", ele pode mudar somente o **Alvo** e os painéis **Agendar** de uma tarefa Pública.
- Se usuário tem direitos "Distribuição" e direitos "Editar Público", ele pode fazer qualquer mudança em tarefas Públicas e pode mudar tarefas de e para a folder Pública.
- Se o usuário tem direitos "Editar Público", mas não tem direitos de "Distribuição", ele não pode editar nenhuma tarefa desse tipo, inclusive tarefas Públicas.

Criação de escopos

Um escopo define os dispositivos que podem ser exibidos e gerenciados por um usuário do Management Suite.

Um escopo pode ter o tamanho que você desejar, abrangendo todos os dispositivos gerenciados analisados em um banco de dados núcleo, ou, possivelmente, apenas um único dispositivo. Essa flexibilidade, aliada ao acesso modular à ferramenta, é o que torna a administração com base em funções um recurso de gerenciamento tão versátil.

Escopos padrão

A administração com base em funções do Management Suite contém um escopo padrão. "Todas as máquinas." Esse escopo inclui todos os dispositivos gerenciados no banco de dados. Não é possível editar ou remover o escopo padrão.

Escopos personalizados

Há três tipos de escopos personalizados que podem ser criados e atribuídos a usuários:

- **Consulta LDMS:** Controla o acesso somente aos dispositivos que correspondam a uma consulta personalizada. É possível selecionar uma consulta existente ou criar novas consultas na caixa de diálogo Propriedades de escopo, para definir um escopo. Observe que você também pode copiar consultas dos grupos **Consultas** na tela de rede diretamente para o grupo **Escopos**. Para obter mais informações sobre consultas, leia ""Gerenciador de diretórios/consultas" na página 183".
- **LDAP:** Controla o acesso somente aos dispositivos obtidos pelo analisador de inventário, localizados em uma estrutura de diretórios compatível com LDAP. Selecione os locais de diretório na caixa de diálogo **Selecionar os dispositivos visíveis** para definir um escopo. Esse tipo de escopo baseado em diretório também suporta locais de diretório personalizado (se tiver digitado caminhos de diretório personalizado como parte da configuração do agente). Os caminhos de diretórios personalizados disponíveis são exibidos na caixa de diálogo **Selecionar os dispositivos visíveis**. Use diretórios personalizados para definir um escopo se não tiver uma estrutura compatível com LDAP ou se desejar restringir o acesso a dispositivos por um detalhe organizacional específico como local geográfico ou departamento.
- **Grupo de dispositivos:** Controla acesso apenas aos grupos de dispositivos na tela de rede.

Um usuário do Management Suite pode ser atribuído a um ou mais escopos por vez. Além disso, um escopo pode ser associado a múltiplos usuários.

Como funcionam escopos múltiplos

É possível atribuir mais de um escopo a qualquer dos usuários do Management Suite. Quando múltiplos escopos são atribuídos a um usuário, o usuário tem direitos em todos os computadores em todos os escopos atribuídos. A lista acumulativa de computadores em todos os escopos atribuídos é o escopo efetivo do usuário.

O escopo efetivo de um usuário pode ser personalizado através da adição ou remoção de escopos a qualquer momento. Múltiplos escopos e tipos de escopo podem ser usados em conjunto.

Os direitos e escopos de um usuário podem ser modificados a qualquer momento. Se você modificar os direitos ou escopos de um usuário, essas mudanças entram em efeito da próxima vez que o usuário acessar o console ou quando administrador do console clicar no botão da barra de ferramentas **Atualizar escopo** no Console (no topo da janela).

Criar um escopo

Um escopo define os dispositivos que podem ser exibidos e gerenciados por um usuário do Management Suite.

Um escopo pode ter o tamanho que você desejar, abrangendo todos os dispositivos gerenciados analisados em um banco de dados núcleo, ou, possivelmente, apenas um único dispositivo.

Para criar um escopo:

1. Clique em **Ferramentas > Administração > Gerenciamento de usuários**.
2. Clique com o botão direito em **Escopos** e clique em **Novo escopo**.
3. Na caixa de diálogo **Propriedades do escopo**, digite o nome do novo escopo.
4. Especifique o tipo de escopo que deseja criar (consulta LDMS, LDAP ou diretório personalizado ou grupo de dispositivos) clicando no tipo de escopo na lista suspensa e clicando em **Novo**.
5. Se estiver criando um escopo baseado em consulta LDMS, defina a consulta na caixa de diálogo **Consulta de novo escopo** e, em seguida, clique em **OK**.
6. Se você estiver criando um escopo baseado em diretório, selecione os locais (diretório LDAP e/ou diretório personalizado) na lista **Selecionar dispositivos visíveis** (você pode procurar no diretório clicando em **Procurar diretórios**) e em seguida em **OK**.

Clique nos sinais de mais (+) e menos (-) para expandir e recolher os nós da árvore de diretório. Todos os nós sob um nó-pai selecionado serão adicionados ao escopo.

Os locais de diretórios LDAP são determinados pela localização do serviço de diretório do dispositivo. Os locais personalizados dos diretórios são determinados pelo atributo de localização do computador de um dispositivo no banco de dados de inventário. Esse atributo é definido durante a configuração do agente do dispositivo.

7. Se estiver criando um escopo baseado em um grupo de dispositivos, selecione um item na lista de grupos de dispositivos disponíveis e clique em **OK**.
8. Clique em **OK** novamente para salvar o escopo e fechar a caixa de diálogo.

Para criar um filtro baseado em uma consulta existente.

1. Clique com o botão direito em **Escopos** e clique em **Novo escopo a partir de uma busca**.
2. Adicione os dispositivos que desejar e clique em **OK**.
3. Uma cópia da consulta será feita e um novo escopo será exibido na árvore com um nome baseado na nome da consulta de origem.

NOTA: Você pode criar um escopo rapidamente a partir de uma consulta existente arrastando uma consulta da Tela de rede e soltando-a na árvore de escopos.

NOTA: Os escopos usam uma cópia da consulta na qual uma cópia da consulta na qual são baseados. Alterações na consulta de origem na Tela de rede não afetará os escopos existentes.

Sobre a caixa de diálogo Propriedades do escopo

Use essa caixa de diálogo para criar ou editar um escopo. É possível acessar essa caixa de diálogo selecionando um escopo e clicando no botão da barra de ferramentas **Editar escopo** ou clicando com o botão direito do mouse no escopo e, em seguida, clicando em **Propriedades**.

- **Nome do escopo:** identifica o escopo.
- **Selecione um tipo de escopo:**
  - **Consulta LDMS:** cria um escopo, cujo intervalo de dispositivos é determinado por uma consulta personalizada. A opção **Novo** com esse tipo de escopo selecionado abre a caixa de diálogo **Nova consulta** onde é possível definir e salvar uma consulta. Essa é a mesma caixa de diálogo de consulta usada na criação de uma consulta de banco de dados da tela de rede. (Observe que você também pode copiar consultas dos grupos de **Consultas** na tela de rede diretamente para o grupo **Escopos**.)
  - **LDAP:** cria um escopo, cujo intervalo de dispositivos é determinado pelo local do dispositivo (diretório LDAP e/ou diretório personalizado). A opção **Novo** com esse tipo de escopo selecionado abre a caixa de diálogo **Selecionar os dispositivos visíveis**, onde é possível selecionar locais a partir dos dados do inventário. Clique nos sinais de mais (+) e menos (-) para expandir e recolher os nós da árvore de diretório. Vários locais podem ser selecionados, usando a combinação Ctrl+clique do mouse Todos os nós sob um nó-pai selecionado serão adicionados ao escopo. Ao clicar em **Procurar diretórios**, você pode procurar e selecionar diretórios na própria árvore do diretório LDAP para os diretórios que você configurou.
  - **Grupo de dispositivos:** cria um escopo cujo intervalo de dispositivos é determinado por um grupo de dispositivos existentes no objeto Dispositivos na tela de rede. Clicar em **Novo** com esse tipo de escopo selecionado abrirá a caixa de diálogo **Filtro de consulta**, onde é possível selecionar um grupo de dispositivos.
- **Definição do escopo atual:** exibe as instruções de consulta para um escopo com base em consultas, os caminhos do local de um escopo com base em diretórios ou o nome do grupo de um escopo com base em grupos de dispositivos.
- **Editar:** abre a caixa de diálogo adequada do escopo onde é possível mudar os parâmetros e as declarações das consultas.

Criar uma equipe

Uma equipe de administração baseada em funções é um grupo de usuários que pode ver e compartilhar a propriedade de tarefas e configurações que pertencem à equipe.

Para criar uma equipe

1. Na ferramenta **Gerenciamento de usuários**, clique com o botão direito em **Equipes** e clique em **Nova equipe**.
2. Digite um **Nome** de equipe.
3. Selecione os **Usuários** e **Grupos** que você deseja na equipe.
4. Clique em **OK**.

Uso de equipes

Uma equipe de administração baseada em funções é um grupo de usuários que pode ver e compartilhar a propriedade de tarefas e configurações que pertencem à equipe. Por exemplo, se você tiver múltiplos departamentos que querem compartilhar consultas ou tarefas, você pode agrupar os departamentos em uma equipe. As tarefas e configurações de uma equipe aparece em um grupo especial com nome da equipe na tela de árvore de uma ferramenta. Por exemplo, se você tivesse uma equipe denominada "Salt Lake" da qual é membro, veria um subgrupo "Dispositivos de 'Salt Lake'" no grupo **Dispositivos** na **Tela da rede**. As pessoas podem pertencer a múltiplas equipes.

As pessoas que não fazem parte de uma equipe em particular não verão o grupo daquela equipe em nenhum lugar no console. As pessoas com direito de administrador verão as equipes e o conteúdo das mesmas. Embora você possa usar pastas públicas para compartilhar conteúdo do console, o conteúdo da pasta pública é visível a todos que tiverem direitos a uma ferramenta. A vantagem das equipes é que somente os membros da equipe vêm o conteúdo da equipe, potencialmente tornando o conteúdo mais organizado e acessível aos membros da equipe.

As equipes consistem em uma ou mais permissões de grupo. Você pode até mesmo criar equipes com 1 ou 2 pessoas. Por exemplo, se uma pessoa estiver doente você pode adicionar o substituto dessa pessoa à mesma equipe. Ou, se tiver duas pessoas que compartilham responsabilidades, você pode colocá-las na mesma equipe.

Administradores e membros da equipe podem mudar a propriedade de itens da árvore clicando com o botão direito e clicando em **Info**. As caixas de diálogo de informações têm uma lista suspensa **Proprietário** onde você pode selecionar o proprietário do item.

Uso de restrições de tempo do controle remoto

O controle remoto limita as horas e dias que os usuários de console podem iniciar sessões de controle remoto. É possível especificar os dias da semana e a hora de início e término (em formato UTC) que você deseja permitir o controle remoto.

Observe que a hora de início está no formato UTC (Hora Coordenada Universal ou Horário Médio de Greenwich). O servidor núcleo determina a hora de início verificando a hora UTC informada pelo sistema operacional do servidor núcleo. O servidor núcleo não faz ajuste para o fuso horário local do usuário do console. Ao inserir a hora inicial, você precisa compensar a diferença entre a hora UTC e o fuso horário local do operador do console e utilizar a hora ajustada resultante.

Por padrão, nenhum limite de tempo do controle remoto está ativa.

Observe que as permissões RBA (do inglês Rights Based Approach - Abordagem baseada em permissões).são aditivas. Se um usuário é membro de múltiplas funções, você poderia permitir involuntariamente o controle remoto quando sua intenção foi de restringi-lo.

Por exemplo, se um usuário é membro de uma função de controle remoto que inclui limites de tempo e o mesmo usuário é membro de uma função de segurança que não inclui limites de tempo, este usuário não terá nenhum limite de tempo de controle remoto.

Para garantir que os limites de tempo do controle remoto sejam aplicados da maneira desejada, certifique-se que somente uma função seja atribuída ao usuários com limites de tempo.

Atribuir restrições de tempo do controle remoto

O controle remoto limita as horas e dias que os usuários de console podem iniciar sessões de controle remoto.

Para usar os limites de tempo do controle remoto

1. Na ferramenta Gerenciamento de usuário (**Ferramentas > Administração > Gerenciamento de usuário**), clique com o botão direito na árvore **Usuários e grupos** e em **Propriedades**.
2. No painel à esquerda, clique em **Limites de tempo do CR**.
3. Selecione **Usar limites de tempo**
4. Selecione os dias nos quais você deseja ativá-lo.
5. Insira o intervalo de horas UTC nos quais você deseja permitir o controle remoto.
6. Clique em **OK** ao terminar.

Configuração do núcleo

Escolha do hardware do servidor do núcleo e do banco de dados

Ao configurar um servidor núcleo LANDesk Management Suite é necessário tomar determinadas decisões quanto à velocidade, memória e armazenamento dos servidores em questão. O administrador precisa também decidir quando mudar de um para múltiplos servidores núcleo. Esta seção trata dessas tomadas de decisão. As quatro escolhas principais de hardware a serem feiras são CPU, memória, armazenamento e placa de rede. As listas que seguem contêm recomendações sobre hardware para vários números de nós gerenciados.

O fator mais importante na tomada dessas decisões será o número de nós gerenciados na rede. O número de nós já deve ter sido estimado durante a coleta de informações sobre a rede. Entretanto, outros fatores como, que componentes serão mais usados, o número de pessoas que precisará ter acesso ao console LANDesk ou ao Web console, o modelo de gerenciamento de rede e conformidade com as práticas e padrões de negócio devem ser considerados.

As recomendações de hardware são diferentes para cada ambiente e as seguintes são diretrizes gerais para ajudar a determinar o hardware ideal para um dado ambiente.

Abaixo as opções para a escolha de software compatível com banco de dados:

- Microsoft SQL Express 2008 (incluído com a Management Suite, recomendado somente para ambientes de teste ou pequenas distribuições)
- Microsoft SQL 2005
- Microsoft SQL 2008
- Oracle 11g R2

Configurações de servidor núcleo único

Todos os serviços do Management Suite hospedados em um servidor (até 750 dispositivos)

Para domínios de gerenciamento do Management Suite com 750 dispositivos ou menos, é possível instalar o servidor núcleo, o console, o servidor de Web Console e o banco de dados núcleo em um único servidor. Nessa situação, pode-se considerar o uso do banco de dados padrão SQL Express, que geralmente é mais fácil de manter. O servidor deve atender pelos menos a estes requisitos de sistema para você instalar o Management Suite em uma configuração 1.000 dispositivos ou menos.

- Processador Intel Xeon Dual Core de 32 bits ou de 64 bits
- 4 GB de RAM
- Adaptador de rede 100/1000 Megabit
- 72 GB de espaço livre em unidades de disco de 10.000 RPM ou mais velozes, ou em matrizes

IMPORTANTE: O Microsoft SQL Express tem um limite de tamanho para o banco de dados de 4 gigabytes. Se esta limite for atingido, o núcleo servidor para de funcionar corretamente e o banco de dados não

conseguirá mais gravar dados. É possível a cada agente usar de 2 a 4 megabytes ou mais, portanto tenha o cuidado de monitorar com atenção o uso do disco e de fazer o upgrade para uma versão completa do SQL antes de atingir o limite de 4 gigabytes.

Configuração de servidor único (de 750 a 1.500 dispositivos)

Se o domínio de gerenciamento do Management Suite consiste em 750 a 1.500 dispositivos, ainda é possível utilizar um único servidor. O servidor devem atender pelo menos aos seguintes requisitos de sistema antes da instalação do Management Suite.

- Processador Intel Xeon Dual Core de 64 bits
- 4 GB ou mais de RAM
- Um adaptador de rede gigabit
- 3 unidades ou matrizes com 72 GB de espaço livre por matriz em discos com 15.000 RPM ou mais velozes

NOTA: Um servidor núcleo gerencia 750 a 1.500 nós executando todos os recursos LANDesk pode experimentar alguma lentidão de leitura/gravação nas unidades se o sistema operacional, o aplicativo LANDesk Management Suite, o banco de dados e os logs do banco de dados estiverem todos na mesma unidade de disco ou matriz. Pode ser necessário um ajuste. Recomenda-se que o servidor que hospedar uma configuração completa como esta tenha três matrizes de unidade de disco em rotores separados (discos físicos) a fim de prevenir a ocorrência de problemas de recursos. A seguinte configuração de unidade de disco deve ser implementada.

- Uma unidade ou matriz para o sistema operacional
- Uma unidade ou matriz para o aplicativo LANDesk Management Suite e o aplicativo do banco de dados
- Uma unidade ou matriz para o banco de dados e os logs do banco de dados

NOTA: O servidor que hospedar essa configuração precisará de três matrizes de unidades em eixos separados (discos físicos).

Configuração de servidor único (de 1.500 a 3.000 dispositivos)

Se o domínio de gerenciamento do Management Suite consiste em 750 a 1.500 dispositivos, ainda será possível utilizar um único servidor. O servidor devem atender pelo menos aos seguintes requisitos de sistema antes da instalação do Management Suite.

- Processadores dual (dois processadores físicos) Intel Xeon Quad Core de 64 bits
- De 6 a10 GB ou mais RAM (4 GB apra o SO e os serviços LANDesk mais de 1 a 2 MB por nó para o banco de dados. Para reserva de RAM, instale 10 GB)
- Importante: O servidor núcleo do Management Suite nessa configuração requer duas matrizes de unidade em eixos separados.
- Um adaptador de rede gigabit
- 3 unidades ou matrizes com 72 GB de espaço livre por matriz em discos com 15.000 RPM ou mais velozes

NOTA: Um servidor núcleo que gerencia 1.500 a 3.000 nós e executa todos os recursos LANDesk pode experimentar alguma lentidão de leitura/gravação nas unidades se o sistema operacional, o aplicativo LANDesk Management Suite, o banco de dados e os logs do banco de dados estiverem todos na mesma unidade de disco ou matriz. Pode ser necessário um ajuste. Recomenda-se que o servidor que hospedar uma configuração completa como esta tenha três matrizes de unidade de disco em rotores separados (discos físicos) a fim de prevenir a ocorrência de problemas de recursos. A seguinte configuração de unidade de disco deve ser implementada.

- Uma matriz para o sistema operacional, Raid 0, 1, 5 ou tecnologia equivalente ou mais rápida
- O software do Management Suite deve ser instalado em uma matriz no RAID 0, 5, 10 uma tecnologia equivalente ou mais rápida
- Uma matriz para o banco de dados e logs do banco de dados, RAID 0, RAID 5 ou RAID 10 ou uma tecnologia equivalente ou mais rápida

IMPORTANTE: O servidor que hospedar essa configuração precisará de três matrizes de unidades em eixos separados (discos físicos).

Configurações de núcleo com multiservidores

Configuração de multiservidores (de 3.000 a 5.000 dispositivos)

Se o domínio de gerenciamento do Management Suite consiste em 3.000 a 5.000 dispositivos, a LANDesk recomenda a divisão dos seus componentes do Management Suite entre dois servidores para melhorar o desempenho. Os servidores devem atender pelo menos aos seguintes requisitos de sistema antes da instalação do Management Suite.

Servidor núcleo do Management Suite e software do Web Console em um único servidor

- Processadores dual (dois processadores físicos) Intel Xeon Quad Core de 64 bits
- 4 GB ou mais de RAM
- Um adaptador de rede gigabit (o núcleo e banco de dados devem ter uma conexão gigabit entre si)
- Duas matrizes com 72 GB de espaço livre por matriz em unidades de disco com 15.000 RPM ou mais velozes
- A matriz do sistema operacional deve ser RAID 0 ou 1 ou uma tecnologia equivalente ou mais rápida
- O software do Management Suite deve ser instalado em uma matriz no RAID 0, 5 ou 10 uma tecnologia equivalente ou mais rápida

Banco de dados núcleo em um segundo servidor

- É recomendado um sistema operacional de 64 bits para o servidor do banco de dados para o gerenciamento de memória

IMPORTANTE: Se estiver usando um sistema operacional Windows Server de 32 bits com SQL, é necessário habilitar AWE (Addressing Windowing Extensions).

- Processadores dual (dois processadores físicos) Intel Xeon Quad Core de 64 bits
- De 4 GB a 10 GB ou RAM (1 GB para o SO, mais de 1 a 2 MB por nó.)

IMPORTANTE: O requisito de RAM varia. Multiplique o total de dispositivos que esse servidor núcleo gerenciará por 2 MB para obter uma estimativa mais precisa. Por exemplo, 5.000 dispositivos requerem de 6 a 10 GB de RAM.

- SQL 2005 ou 2008 Enterprise ou Oracle 11 g
- Três matrizes com 72 GB de espaço livre por matriz em unidades de disco com 15.000 RPM ou mais velozes
- A matriz do sistema operacional deve ser RAID 1 ou uma tecnologia equivalente ou mais rápida
- Uma matriz para o banco de dados, RAID 0, RAID 5 ou RAID 10 ou uma tecnologia equivalente ou mais rápida
- Uma matriz para os logs do banco de dados, RAID 0,1, 5 ou uma tecnologia equivalente ou mais rápida

IMPORTANTE: O servidor do banco de dados dessa configuração requer três matrizes de unidade em eixos separados:

- Um adaptador de rede gigabit (o núcleo e banco de dados devem ter uma conexão gigabit entre si)

Configuração de multiservidores (5.000-8.000 dispositivos)

Se o domínio de gerenciamento do Management Suite consiste em 5.000 a 8.000 dispositivos, a LANDesk recomenda a divisão dos seus componentes do Management Suite entre dois servidores para melhorar o desempenho. Os servidores devem atender pelo menos aos seguintes requisitos de sistema antes da instalação do Management Suite.

Servidor núcleo do Management Suite e software do Web Console em um único servidor

- Processadores Quad (quatro processadores físicos) Intel Xeon Quad Core de 64 bits

IMPORTANTE: Se estiver usando um sistema operacional Windows Server de 32 bits com SQL, é necessário habilitar AWE (Addressing Windowing Extensions).

- 4 GB ou mais de RAM

IMPORTANTE: O servidor núcleo do Management Suite nessa configuração requer duas matrizes de unidade em eixos separados.

- Duas matrizes com 72 GB de espaço livre por matriz em unidades de disco com 15.000 RPM ou mais velozes
- A matriz do sistema operacional deve ser RAID 1 ou uma tecnologia equivalente ou mais rápida
- O software do Management Suite deve ser instalado em uma matriz no RAID 0, 1, 5 ou 10 ou uma tecnologia equivalente ou mais rápida
- Um adaptador de rede gigabit (o núcleo e banco de dados devem ter uma conexão gigabit entre si)

Banco de dados núcleo em um segundo servidor

- É recomendado um sistema operacional de 64 bits para o servidor do banco de dados para o gerenciamento de memória
- Processadores dual (dois processadores físicos) Intel Xeon Quad Core de 64 bits
- De 6 GB a 12 GB ou RAM (1 GB para o SO, mais de 1 a 2 MB por nó.)

IMPORTANTE: O requisito de RAM varia. Multiplique o total de dispositivos que esse servidor núcleo gerenciará por 2 MB para obter uma estimativa mais precisa. Por exemplo, 8.000 dispositivos requerem de 9 a 16 GB de RAM.

- SQL 2005 ou 2008 Enterprise ou Oracle 11 g
- Três matrizes com 72 GB de espaço livre por matriz em unidades de disco com 15.000 RPM ou mais velozes
- A matriz do sistema operacional deve ser RAID 1 ou uma tecnologia equivalente ou mais rápida
- Uma matriz para o banco de dados, RAID 0, RAID 5 ou RAID 10 ou uma tecnologia equivalente ou mais rápida
- Uma matriz para os logs do banco de dados, RAID 0,1, 5 ou uma tecnologia equivalente ou mais rápida

IMPORTANTE: O servidor do banco de dados dessa configuração requer três matrizes de unidade em eixos separados:

- Um adaptador de rede gigabit (o núcleo e banco de dados devem ter uma conexão gigabit entre si)

Configuração de multiservidores (8.000-16.000 dispositivos)

Se o domínio de gerenciamento do Management Suite consiste em 8.000 ou mais dispositivos, a LANDesk recomenda a divisão dos seus componentes do Management Suite entre dois servidores para melhorar o desempenho em todas as áreas. Os servidores devem atender pelo menos aos seguintes requisitos de sistema antes da instalação do Management Suite.

Servidor núcleo do Management Suite e software do Web Console em um único servidor

- Quatro processadores físicos, cada um sendo dual-core ou superior
- De 4 a 8 GB de RAM
- Duas matrizes com 72 GB de espaço livre por matriz em unidades de disco com 15.000 RPM ou mais velozes
- A matriz do sistema operacional deve ser RAID 1 ou uma tecnologia equivalente ou mais rápida
- O software do Management Suite deve ser instalado em uma matriz no RAID 0, 1, 5 ou 10 ou uma tecnologia equivalente ou mais rápida

IMPORTANTE: O LANDesk executa muitas operações de gravação nas seguintes pastas no diretório LDLogon: LDScan, VulscanResults, sdstatus, AlertQueue, etc. Montar uma unidade como uma pasta como LDlogon em vez de uma letra de unidade pode melhorar a E/S do disco.

IMPORTANTE: O servidor núcleo do Management Suite nessa configuração requer duas matrizes de unidade em eixos separados.

- A matriz do sistema operacional deve ser RAID 1 ou uma tecnologia equivalente ou mais rápida
- A matriz do aplicativo deve estar em uma segunda matriz RAID separada
- Um adaptador de rede gigabit (o núcleo e banco de dados devem ter uma conexão gigabit entre si)

Banco de dados núcleo em um segundo servidor

- É recomendado um sistema operacional de 64 bits para o servidor do banco de dados para o gerenciamento de memória

IMPORTANTE: Se estiver usando um sistema operacional Windows Server de 32 bits com SQL, é necessário habilitar AWE (Addressing Windowing Extensions).

- Processadores quad (quatro processadores físicos) Intel Xeon Quad Core de 64 bits
- Mínimo de 12 GB a 24 GB de RAM.

IMPORTANTE: O requisito de RAM varia. Multiplique o número de dispositivos que esse servidor núcleo gerenciará por 1 ou 2 MB para obter uma melhor estimativa. Por exemplo, 16.000 dispositivos requerem de 17 a 24 GB de RAM.

- SQL 2005 ou 2008 Enterprise ou Oracle 11 g
- Três matrizes com 72 GB de espaço livre por matriz em unidades de disco com 15.000 RPM ou uma tecnologia equivalente ou mais rápida
- A matriz do sistema operacional deve ser RAID 1 ou uma tecnologia equivalente ou mais rápida
- Uma matriz para o banco de dados, RAID 0, RAID 5 ou RAID 10 ou uma tecnologia equivalente ou mais rápida
- Uma matriz para os logs do banco de dados, RAID 0,1 ou 5 ou uma tecnologia equivalente ou mais rápida
- Um adaptador de rede gigabit (o núcleo e banco de dados devem ter uma conexão gigabit entre si)

Configuração de multiservidores (16.000 dispositivos ou mais)

Com nossos novos recursos de núcleo Enterprise o LANDesk oferece suporte à servidores núcleo únicos que excedem 16.000 nós. Para as instalações do LANDesk Management Suite deste tamanho e maior nós recomendamos obter mais assistência para o ajuste com os Serviços Profissionais LANDesk (LANDesk Professional Services) ou um ESP (Expert Solutions Provider [Provedor de soluções especializadas]).

Executar a instalação do LANDesk Management Suite

Antes de instalar o Management Suite, verifique se o servidor que escolheu atende aos requisitos do sistema descritos anteriormente nesta seção. As seguintes são as etapas para a instalação do Management Suite com o banco de dados Microsoft SQL Express 2008. Se você for usar um dos outros bancos de dados suportados, é necessário instalar e configurar o banco de dados antes de executar a instalação do Management Suite. As instruções detalhadas sobre como fazer isso e instalar o Management Suite estão disponíveis na Comunidade do usuário do LANDesk http://support.landesk.com.

O serviço de indexação e o serviço de pesquisa do Windows precisam ambos ser desativados antes da instalação do LANDesk Management Suite 9.5; se isso não for feito a instalação pode falhar. Consulte o seguinte artigo para encontrar mais informações: http://community.landesk.com/support/docs/DOC-7245.

Certifique-se também de que o servidor onde você está executando a instalação não tem o Serviço de atualização do Windows Server instalado. Se este serviço estiver ativo você terá problemas para fazer o logon no console.

Como cada ambiente tem necessidades diferentes recomendamos contatar o seu revendedor ou o provedor ESP (Expert Solution Provider) sobre Certified LANDesk Deployment. Se você não tiver certeza de quem é o seu revendedor, visite este site para encontrar um gerente de vendas na LANDesk o qual pode indicar quem é o seu revendedor:

- http://www.landesk.com/wheretobuy/default.aspx

Mais informações estão disponíveis no site a seguir:

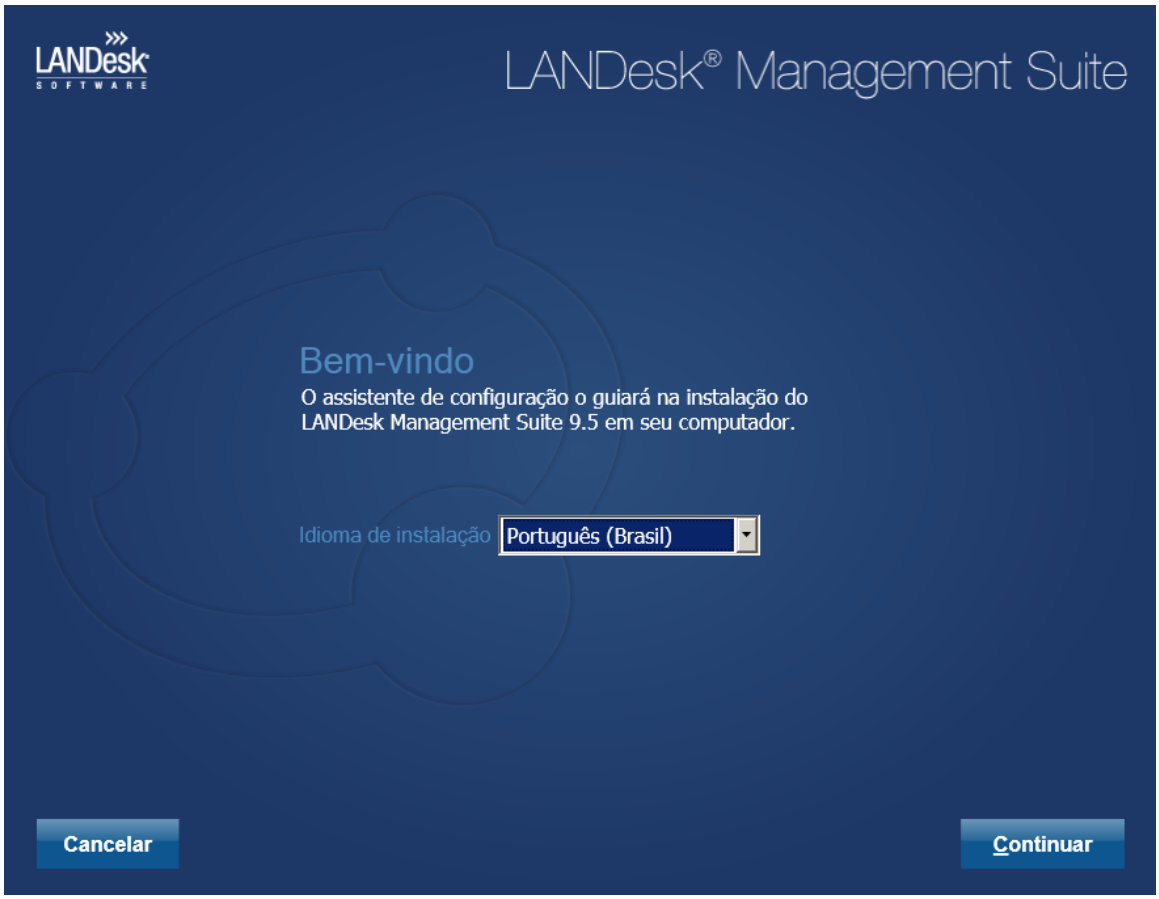
- http://www.landesk.com/SupportDownload/Support.aspx?id=3215

A configuração do Management Suite abrirá portas do Windows Firewall no servidor núcleo. Normalmente, a configuração do Management Suite e do agente configuram as portas automaticamente. Se você estiver usando um firewall diferente a configuração das portas deverá ser feita manualmente. Para obter mais informações sobre as portas que o Management Suite usa, consulte os sites:

- Portas usadas pelo LANDesk Management Suite - Lista completa: http://community.landesk.com/support/docs/DOC-1591

Para instalar o LANDesk Management Suite

1. Na sua mídia de instalação, abra o Setup.exe.



2. Na tela principal de boas vindas, selecione um idioma para instalação e clique em **Continuar**.
3. Aceite o Contrato de licença e clique em **Avançar**.
4. Na página **O que você quer instalar,** certifique-se de que o **Servidor núcleo** está selecionado e clique em **Continuar.**
5. Na página **Pré-requisitos**, assegure-se de que o seu servidor se conforma aos pré-requisitos. Caso contrário, instale os pré-requisitos faltantes e clique em **Continuar**.
6. Na página **Como a LANDesk deve configurar seu banco de dados**, clique em **Configurar um novo banco de dados 9.5** e em **Continuar**.
7. Na página **Aplicativo do banco de dados**, selecione **SQL Express (Agrupado)** e clique em **Continuar**.
8. Na página **Onde você quer instalar**, clique em **Continuar** para aceitar o caminho padrão de instalação (C:\Arquivos de programas (x86)\LANDesk\ManagementSuite\).
9. Na página **Pronto para instalar**, clique em **Instalar**.
10. Ao terminar configuração, clique em **Reiniciar agora**.
11. Após a reinicialização, aguarde cinco minutos para todos os serviços iniciarem.
12. Ativa seu núcleo como descrito em "Ativação do servidor núcleo" na página 71.
13. Abra o console e acesse com as credenciais de Windows do usuário conectado durante a instalação do . (Durante a instalação, esse usuário recebe automaticamente direitos plenos de administrador no console.)

Quando você abre o console, aparece um assistente de início que o ajuda a configurar o Management Suite. é importante que você execute essas etapas. Após ter feito isso, consulte "Configuração de agentes de dispositivo" na página 99 e a Comunidade de usuários LANDesk http://community.landesk.com para encontrar mais informações sobre a distribuição de agentes.

Configurar consoles Management Suite adicionais

O console do Management Suite é automaticamente instalado no servidor núcleo. Este console deve ser instalado nos computadores do administrador LANDesk que precisam de funcionalidade total ou acesso a todas as ferramentas Management Suite. O console é usado para interagir com os vários recursos do Management Suite; por exemplo, para distribuir software, controlar remotamente dispositivos gerenciados, ver as informações de inventário e executar outras funções de gerenciamento.

Para mais utilidade e funcionalidade, os consoles podem ser instalados na rede inteira. (A LANDesk Software não cobra nenhuma taxa adicional pelos consoles.)

Para obter mais informações sobre plataformas compatíveis, consulte este documento na comunidade de usuários da LANDesk: http://community.landesk.com/support/docs/DOC-7478.

Para instalar um console adicional

1. Da mídia de instalação do Management Suite, abra a execução automática (autorun).
2. Clique no botão **Console remoto**.
3. Clique em **Continuar**.
4. Se a verificação de pré-requisito for aprovada, clique em **Continuar**. Caso contrário, corrija os pré-requisitos faltantes.
5. Clique em **Executar configuração**.
6. Siga os avisos de instalação.

Configuração do Console Web

O console Web oferece um subconjunto de funcionalidades do console Management Suite que pode ser utilizado com conveniência de um navegador. Quando instalado em um servidor de web, os usuários designados podem acessá-lo através do Microsoft Internet Explorer ou de outros navegadores suportados. Esta configuração (instalada como padrão no servidor núcleo) permite o acesso ao console Web por usuários sem instalação adicional em seus PCs locais.

Como padrão, a instalação coloca os arquivos do Web Console na pasta \Inetpub\wwwroot\remote.

A configuração também cria arquivos compartilhados do Web console com as permissões necessárias no servidor núcleo.

O Web console e os dispositivos gerenciados precisam os seguintes compartilhamentos e permissões para funcionarem corretamente:

- **ldmain:** Aplicativos de servidor (\Arquivos de programas\LANDesk\ManagementSuite). O grupo Administradores deve ter Controle total. Para o Microsoft Windows 2003, o grupo Serviço de rede precisa ter os direitos de Leitura e Execução, Listar conteúdo de pasta e Leitura.
- **ldlog:** Logs (\Arquivos de programas\LANDesk\ManagementSuite\log).

- **ldlogon:** Aplicativos de dispositivo gerenciado e agentes (\Arquivos de programas\LANDesk\ManagementSuite\ldlogon). O grupo Administradores precisa ter os direitos Controle total e o grupo Todos deve ter direitos de Somente leitura.
- **scripts:** Scripts de distribuição de software (\Arquivos de programas\LANDesk\ManagementSuite\Scripts).

Se o console Web estiver sendo instalado em um servidor diferente do núcleo, o usuário conectado precisa ser um administrador de domínio e a conta de administrador de domínio precisa estar em um dos grupos de usuários LANDesk do servidor de núcleo. Os servidores do núcleo e do Web console devem estar no mesmo domínio, e os usuários que precisar usar o Web console precisam ser adicionados a um dos grupos de usuários do LANDesk Management Suite ou o servidor núcleo e o servidor do Web console.

O Web console do Management Suite 9 não pode ser executado em um servidor núcleo ou de console mais antigo. Somente o Web console do Management Suite 9 pode ser executado em um servidor núcleo do Management Suite 9 ou um computador de console. Versões anteriores do Management Suite não funcionarão.

Se o console Web estiver sendo instalado em um servidor Microsoft Windows 2003, o IIS (Internet Information Server) desativa as páginas ativas de servidor (ASP) como padrão. Elas precisam ser ativadas para que o Web console funcione corretamente.

Para ativar as páginas páginas ativas de servidor (ASP) em servidores Microsoft Windows 2003

1. Clique em **Iniciar | Ferramentas administrativas | Internet Information Services (IIS) Manager**.
2. Clique para expandir <CoreServerName>.
3. Clique em **Extensão de serviço de web**.
4. Clique em **Active Server Pages** (Páginas ativas de servidor).
5. Clique em **Permitir**.
6. Feche a janela do Gerenciador do IIS (Internet Information Services).

Para verificar a instalação do Web Console, abra um navegador e digite um URL de servidor de web. Com padrão o URL é:

- http://<WebServerName>/remote

A instalação foi correta se o navegador solicitar as credenciais de login e abrir o console.

A primeira vez que o console é iniciado, ele pode levar até 90 segundos para aparecer na tela. Essa demora ocorre porque o servidor precisa fazer uma compilação inicial de determinados códigos do console. O console iniciará muito mais rápido após a primeira vez.

Se aparecer o erro de permissão quando o console Web estiver sendo acessado, a autenticação integrada do Microsoft Windows precisa estar ativada como método de autenticação para o site do console Web.

Como verificar o método de autenticação

1. Clique em **Iniciar > Ferramentas administrativas > Gerenciador do Internet Information Services (IIS)**
2. Clique para expandir **<CoreServerName> > Sites > Site da web padrão**.
3. Clique em **Propriedades** do menu suspenso da pasta **Remoto**.
4. Clique na guia **Segurança do diretório**.
5. Clique em **Editar** no campo **Acesso anônimo e controle de autenticação**.

6. Desmarque a caixa de seleção **Habilitar acesso anônimo**.
7. Marque a caixa de seleção **Autenticação integrada do Windows**.
8. Clique em **OK** para sair da janela **Métodos de autenticação**.
9. Clique em **OK** para sair da janela **Propriedades remotas**.
10. Feche a janela do Gerenciador do IIS (Internet Information Services).

Comparação entre o console e o console Web

A tabela abaixo contém os recursos do console do Management Suite e do Web console do Management Suite.

Recurso	Console	Console Web	Notas
Configuração de agente	Sim	Mínimo	Tarefas agendadas de Distribuições e atualização de agentes são visíveis e controláveis pelos usuários do Web Console com direitos para Configuração de agentes.
Alertas	Sim	Não	
Antivírus	Sim	Não	
Configuração do conjunto de colunas	Sim	Sim	No acesso do console Web sob Preferências na guia Colunas personalizadas.
Configurar serviços	Sim	Não	
Gerenciador de controle de conexão	Sim	Mínimo	As distribuições agendadas são visíveis e controláveis pelos usuários do Web Console com direitos de CCM.
Formulários de dados personalizados	Sim	Não	
Métodos de entrega	Sim	Sim	Guia localizada em Distribuição no Web Console.
Clique com o botão direito em dispositivo	Sim	Sim	Comportamento muito variado – a única função repetida é a execução de análise de inventário (“Analisar dispositivo” em web).
Gerenciador de diretórios	Sim	Sim	
Gerenciador de tela	Sim	Não	
Pacotes de distribuição	Sim	Sim	
Prevenção de intrusão no host	Sim	Não	

Recurso	Console	Console Web	Notas
Gerenciador de link de LaunchPad	Sim	Mínimo	As Distribuições de link de LaunchPad agendadas são visíveis e controláveis pelos usuários do Web Console com direitos de CCM.
Logs	Sim	Não	
Gerenciar scripts	Sim	Parcial	De scripts, scripts existentes podem ser agendados e agrupados.
Distribuição do SO	Sim	Mínimo	Scripts de distribuição de SO existentes que já foram agendados podem ser vistos e controlados pelos usuários do Web Console com direitos a OSD via Scripts > Scripts OSD.
Gerenciamento de energia	Sim	Mínimo	Tarefas agendadas de diretiva de energia são potencialmente visíveis e controláveis pelos usuários do console Web.
Provisionamento	Sim	Não	
Menu de inicialização de PXE	Sim	Não	
Capacidade de consulta	Sim	Parcial	O console Web permite o uso de um recurso de contagem que não está no console do Windows. As consultas não podem ser visualizadas como relatórios no console Web.
Controle remoto	Sim	Sim	
Relatórios	Sim	Sim	O console de relatório abre-se em uma janela separada do navegador.
Tarefas agendadas	Sim	Sim	
Escopos	Sim	Parcial	Escopos existentes podem ser adicionados a um usuário, mas não é possível criar novos escopos.
Security and Patch Manager	Sim	Mínimo	As tarefas agendadas de análise e reparo são visíveis e controláveis pelos usuários do Web Console com direitos de Gerenciador de patch.
Monitoração de licença de software:	Sim	Parcial	Os dados de uso de produto não são visíveis no console Web, os relatórios individuais de conformidade de produto e grupo não estão disponíveis e você não pode ignorar ou agrupar produtos.
Descoberta de dispositivos não gerenciados	Sim	Mínimo	As distribuições agendadas de Análises de descoberta de dispositivos não gerenciados são visíveis e controláveis pelos usuários do console Web com direitos de UDD.
Usuários	Sim	Não	
Configuração de agente Windows CE	Sim	Não	
Criador de CAB de Windows CE	Sim	Não	

Ativação do servidor núcleo

O LANDesk Software, Inc. usa um servidor de licenciamento central para ajudá-lo a gerenciar as licenças de nós e produtos do seu servidor núcleo. Para usar os produtos LANDesk, você deve obter um nome de usuário e uma senha do LANDesk para ativar o servidor núcleo com o certificado autorizado. A ativação é necessária em cada servidor núcleo antes de você poder usar os produtos no servidor. Você pode ativar cada servidor núcleo automaticamente pela Internet ou manualmente por e-mail. Você pode reativar um servidor núcleo no caso de modificar significativamente a configuração do seu hardware.

Periodicamente, o componente de ativação em cada servidor núcleo gerará dados relativos a:

- O número preciso de nós que você está utilizando
- Configuração do hardware criptografada, que não é de caráter pessoal
- Os programas específicos do Software do LANDesk que você estiver usando (coletivamente denominados "dados de contagem de nós")

Nenhum outro dado é coletado ou gerado pela ativação. O código chave de hardware é gerado no servidor núcleo com o uso de fatores de configuração de hardware não pessoais como, o tamanho do disco rígido, velocidade de processamento do computador, etc. O código chave de hardware é enviado para a LANDesk no formato criptografado e a chave privada para a criptografia reside apenas no servidor núcleo. O código chave de hardware é, então, usado pela LANDesk para criar uma parte do certificado autorizado.

Após instalar um servidor núcleo, use o utilitário Ativação do servidor núcleo (**Iniciar > Todos os programas > LANDesk > Ativação do servidor núcleo**) para ativá-lo com uma conta LANDesk associada às licenças que adquiriu ou com uma licença de avaliação de 45 dias. A licença de avaliação de 45 dias é válida para 100 nós. O período de avaliação de 45 dias começa quando você ativa, inicialmente, um produto no servidor núcleo. Se você instalar outros produtos LANDesk para avaliação no servidor núcleo mais tarde, porém ainda dentro do período de 45 dias, o período de avaliação inicial não será estendido. Todos os produtos LANDesk em um único servidor núcleo compartilham a mesma licença de avaliação e o mesmo período de avaliação de 45 dias.

Você pode instalar produtos LANDesk adicionais sob a licença de avaliação de 45 dias usando o programa de execução automática do CD de instalação. Instale o produto desejado na instalação automática e escolha a opção **Modificar** durante a inicialização. Poderá, dessa maneira, adicionar ou remover produtos LANDesk no servidor núcleo.

Você pode mudar a avaliação de 45 dias para uma licença paga a qualquer momento, através do utilitário de Ativação do servidor núcleo, digitando seu nome do usuário e senha LANDesk.

Há dois tipos de licenças: para clientes e para servidores. Toda vez que você instala agentes Management Suite em um sistema operacional como, por exemplo, Windows 2000 Server ou Windows 2003 Server, essa instalação consome uma licença Management Suitepara um servidor. Os servidores de rollup não precisam ser ativados.

Toda vez que os dados de contagem de nós são gerados pelo software de ativação em um servidor de núcleo, você precisa enviar esses dados para LANDesk, automaticamente pela Internet ou manualmente por e-mail. Se você não fornecer os dados de contagem de nós no prazo de 30 dias após a tentativa inicial de verificação da contagem de nós, o servidor núcleo pode parar de funcionar até que você envie os dados de contagem de nós para o LANDesk. Após os dados de contagem de nós serem enviados, o LANDesk fornece um certificado autorizado que permite ao servidor núcleo retomar seu funcionamento normal.

Depois de ativar o servidor núcleo, use a caixa de diálogo **Configurar > Licenciamento de produtos** do console do Management Suite para ver os produtos e o número de nós autorizados adquiridos para a conta com a qual o servidor se autentica. Você pode também ver a data em que o servidor núcleo verificará os dados de contagem de nós junto ao servidor de licenciamento central. O servidor núcleo não o limita ao número de nós autorizados que você adquiriu.

Sobre o utilitário de Ativação do servidor núcleo

Use o utilitário de Ativação do servidor núcleo para:

- Ativar um novo servidor pela primeira vez
- Atualizar um servidor núcleo ou mudar de uma licença de avaliação para uma licença plena
- Ativar um novo servidor com uma licença de avaliação de 45 dias

Inicie o utilitário clicando em **Iniciar > Todos os programas > LANDesk > Ativação do servidor núcleo**. Se o seu servidor núcleo não tiver conexão com a Internet, consulte "Ativação manual de um núcleo ou verificação manual dos dados de contagem de nós" na página 73.

Cada servidor núcleo deve ter um certificado autorizado exclusivo. Não é possível para vários servidores núcleo compartilhar o mesmo certificado de autorização, embora possam verificar a contagem de nós para a mesma conta LANDesk.

Periodicamente, o servidor núcleo gera informações de verificação de contagem de nós no arquivo "\Arquivos de programa\LANDesk\Authorization Files\LANDesk.usage". Esse arquivo é enviado periodicamente para o servidor de licenciamento da LANDesk. Esse arquivo está em formato XML, é assinado digitalmente e criptografado. Todas as mudanças feitas manualmente neste arquivo invalidam seu conteúdo e também o próximo relatório de utilização para o servidor de licenciamento da LANDesk.

O núcleo se comunica com o servidor de licenciamento da LANDesk via HTTP. Se você usa um servidor proxy, clique na guia **Proxy** do utilitário e digite as informações do seu proxy. Se seu núcleo tem uma conexão com a Internet, a comunicação com o servidor de licenciamento é automática, não exigindo nenhuma intervenção de sua parte.

Observe que o utilitário de Ativação do servidor núcleo não inicia automaticamente uma conexão dial-up à Internet, mas se você iniciar a conexão dial-up manualmente e executar o utilitário de ativação, o utilitário poderá utilizar a conexão dial-up para enviar os dados do relatório de utilização.

Se seu servidor núcleo não dispor de uma conexão com a Internet, você pode verificar e enviar a contagem de nós manualmente, do modo descrito mais adiante nesta seção.

Ativação de um servidor com a conta da LANDesk

Antes de poder ativar um novo servidor com uma licença plena, você deve configurar uma conta LANDesk, que lhe fornece as licenças adquiridas para os produtos LANDesk, e para o número de nós para os quais você tenha adquirido licenças. São necessárias as informações de conta (nome de contato e senha) para ativar seu servidor. Se você não tiver essas informações, contate o seu representante de vendas LANDesk.

Para ativar um servidor

1. Clique em **Iniciar > Todos os programas > LANDesk > Ativação do servidor núcleo**.
2. Clique em **Ativar este servidor núcleousando o nome do contato e a senha do**LANDesk.
3. Digite o **Nome do contato** e a **Senha** que desejar que o núcleo utilize.
4. Clique em **Ativar**.

Ativar um servidor com uma licença de avaliação

A licença temporária de 45 dias ativa seu servidor no servidor de licenciamento do LANDesk. Uma vez esgotado o período de avaliação de 45 dias, você não conseguirá fazer logon no servidor núcleo, e o servidor irá parar de aceitar análises de inventário, mas você não perderá nenhum dos dados existentes no software ou no banco de dados. Durante ou após os 45 dias de validade da licença de avaliação, você pode executar novamente o utilitário de Ativação do servidor núcleo e mudar para a ativação plena que utiliza uma conta do LANDesk. Se a licença de avaliação já estiver vencida, uma mudança para uma licença plena irá reativar o núcleo.

Para ativar uma avaliação de 45 dias

1. Clique em Iniciar > Todos os programas > LANDesk > Ativação do servidor núcleo.
2. Clique em **Ativar este núcleo para uma avaliação de 45 dias**.
3. Clique em **Ativar**.

Atualização de uma conta existente

A opção de atualização envia as informações de uso para o servidor de licenciamento da LANDesk. Os dados da utilização são enviados automaticamente se você tiver uma conexão com a Internet, portanto normalmente você não precisa usar esta opção para enviar a verificação da contagem de nós. Você também pode usar esta opção para mudar a conta LANDesk à qual o servidor núcleo pertence. Esta opção também pode ser usada para mudar um servidor núcleo da licença de avaliação para a licença plena.

Para atualizar uma conta existente

1. Clique em **Iniciar > Todos os programas > LANDesk > Ativação do servidor núcleo**.
2. Clique em **Atualizar este servidor núcleousando o nome do contato e a senha LANDesk**.
3. Digite o **Nome do contato** e a **Senha** que desejar que o núcleo utilize. Se você digitar um nome e senha diferentes daqueles usados originalmente para ativar o núcleo, o núcleo será mudado para uma nova conta.
4. Clique em **Ativar**.

Ativação manual de um núcleo ou verificação manual dos dados de contagem de nós

Se o servidor núcleo não dispor de uma conexão com a Internet, o utilitário de Ativação do servidor núcleo não poderá enviar os dados da contagem de nós. Neste caso, você verá uma mensagem lhe pedindo para enviar os dados de verificação de contagem de nós e de ativação manualmente através de um e-mail. A ativação por e-mail é um processo simples e rápido. Quando você vir a mensagem de ativação manual no núcleo, ou se usar o utilitário de Ativação do servidor núcleo e vir a mensagem de ativação manual, siga os passos a seguir.

Para ativar manualmente um núcleo ou verificar manualmente os dados de contagem de nós

1. Quando o núcleo lhe pedir para verificar manualmente os dados da contagem de nós, ele criará um arquivo de dados chamado {languagecode}-activate.{ datestring}.txt na pasta "\Arquivos de programas\LANDesk\Authorization Files". Anexe esse arquivo a uma mensagem de e-mail e envie-a para licensing@landesk.com. O assunto e o corpo da mensagem não são importantes.

2. O LANDesk processará o anexo da mensagem e enviará uma resposta ao endereço de e-mail do qual a mensagem foi enviada. A mensagem do LANDesk lhe fornecerá instruções e incluirá um novo arquivo de autorização anexado.
3. Salve o arquivo de autorização anexado na pasta "\Arquivos de programas\LANDesk\Authorization Files". O servidor núcleo processará o arquivo imediatamente e atualizará o status da ativação.

Se a ativação manual falhar ou o núcleo não conseguir processar o arquivo de ativação anexado, o arquivo de autorização que você copiou será renomeado com a extensão .rejected, e o utilitário irá registrar um evento com mais detalhes no log do aplicativo do Visualizador de eventos do Windows.

Configuração das credenciais do servidor COM+

Ao usar um servidor de Web console diferente do núcleo ou, se quiser usar grupos de domínio dentro do grupo LANDesk Management Suite no servidor núcleo, é necessário fazer algumas configurações adicionais de servidor a serem feitas para a autenticação do Management Suite funcionar corretamente. Os servidores de Web console devem obter as informações de conexão do banco de dados e as informações do usuário do servidor núcleo, entretanto esses servidores usam credenciais personificadas de Web no IIS, por isso eles não podem comunicar-se com o servidor núcleo diretamente.

Para resolver esse problema, o servidor de Web console e o servidor núcleo usam um aplicativo COM+ para comunicar-se via HTTPS, o que permite ao servidor de Web console obter informações do banco de dados e do usuário. É necessário configurar esse aplicativo COM+ no servidor Web console para usar uma conta com os direitos necessários como, por exemplo, uma conta de administrador de domínio. A conta que for fornecida precisa estar no grupo LANDesk Management Suite no servidor núcleo (isso permite o acesso às informações de conexão do banco de dados do servidor núcleo) e deve ter direitos para enumerar membros de domínio Windows.

Se estiver usando grupos de domínio dentro do grupo LANDesk Management Suite do servidor núcleo, o Management Suite também precisa poder enumerar os membros do domínio also Windows. Nesse caso, é necessário também fornecer uma conta para o aplicativo LANDesk1 COM+ do servidor núcleo.

Para configurar o aplicativo LANDesk1 COM+ em um núcleo ou servidor de Web console remoto

1. Vá para o servidor de Web ou o servidor núcleo que deseja configurar.
2. Nas Ferramentas administrativas do Painel de controle do Windows, abra **Serviços de componente**.
3. Clique em **Serviços de componente > Computadores Meu computador > Aplicativos COM+.**
4. No menu de atalho do aplicativo **LANDesk1** COM+ e selecione **Propriedades**.
5. Na guia **Identidade**, digite as credenciais que quer usar.
6. Clique em **OK**.

Plataformas e funcionalidade suportadas

Para obter mais informações sobre sobre as versões do sistemas operacionais e idiomas suportados pela Management Suite (para o servidor núcleo, dispositivos gerenciados e recursos e ferramentas da LANDesk), veja os seguintes documentos da Comunidade de usuários da LANDesk:

- Plataformas com suporte e Matriz de compatibilidade do LANDesk Management Suite
- Idiomas de cliente com suporte do LANDesk Management Suite

Uso de portas com o Management Suite

Ao usar o Management Suite em um ambiente que inclua firewalls (ou roteadores que filtram tráfego), são necessárias informações sobre que portas precisam ser abertas nas firewalls.

Os seguintes documentos do site da comunidade LANDesk identificam as portas que o Management Suite usa no seu servidor núcleo e dispositivos gerenciados.

- Portas usadas pelo LANDesk Management Suite - Lista completa: http://community.landesk.com/support/docs/DOC-1591
- Diagrama da arquitetura de portas: http://community.landesk.com/support/docs/DOC-8092

IMPORTANTE: Normalmente, a configuração do LANDesk Management Suite e da configuração de agente irão configurar estas portas automaticamente no Firewall do Windows durante o processo de instalação. Se você estiver usando um firewall diferente a configuração das portas deverá ser feita manualmente.

Aprimoramentos de segurança do servidor núcleo

A LANDesk quer ter certeza de que você deposita a máxima confiança na segurança (não apenas dos dispositivos gerenciados e protegidos do usuário final na rede, mas também dos servidores núcleo LANDesk, núcleos de aumento e consoles adicionais).

Com esta última versão, já implementamos diversas medidas críticas que ajudam a cumprir esse objetivo.

Principais recursos de segurança do servidor núcleo introduzidos com a versão 9.5

A versão LANDesk® Management Suite9.5 adiciona diversos novos e inteligentes aprimoramentos de segurança do servidor núcleo LANDesk. Essas melhorias foram projetadas para ajudar os administradores do sistema LANDesk a garantir e proteger mais amplamente seu servidor núcleo na rede — contra ataques de softwares maliciosos, acesso não autorizado e outras exposições de segurança comuns.

Os aprimoramentos de segurança do servidor núcleo não estão localizados em uma única ferramenta, serviço ou interface no console LANDesk; ao contrário, eles estão espalhados por todo o produto. Portanto, para poder compreender, monitorar e acompanhar (se necessário), de maneira mais fácil e rápida, essas importantes atualizações de segurança do servidor núcleo, elas foram consolidadas e descritas aqui em um único tópico da ajuda.

Este tópico relaciona onde estão os aprimoramentos de segurança e os descreve aqui ou fornece um link para o respectivo recurso onde é possível encontrar informações mais detalhadas.

Os seguintes recursos foram adicionados e/ou atualizados a fim de reforçar a segurança do servidor núcleo.

- "O acesso de compartilhamento LDMAIN é restrito" na página 76
- "Aprimoramentos de segurança dos serviços Web e do console Web" na página 77
- "O acesso remoto ao registro está desativado" na página 77
- "Atualizações do Open SSL" na página 78
- "Aprimoramentos do banco de dados criptografados" na página 78
- "Características/itens removidos para aprimorar a segurança do núcleo" na página 79

O acesso de compartilhamento LDMAIN é restrito

A parte de LDMAIN é trancada para baixo. O motivo é impedir que usuários gerais da LANDesk acessem essa pasta onde podem modificar arquivos críticos (por exemplo, arquivos de scripts personalizados).

NOTA: Os scripts personalizados foram movidos
Para evitar o acesso não autorizado, os arquivos de scripts personalizados foram movidos para o banco de dados do núcleo.

A parte de LDMAIN exigiu uma implementação mais segura, e realizar este objetivo que as seguintes mudanças foram feitas:

O LDMAIN foi movido de:

```
C:\Arquivos de Programas (x86)\LANDesk\ManagementSuite (que era o compartilhamento LDMAIN)
```

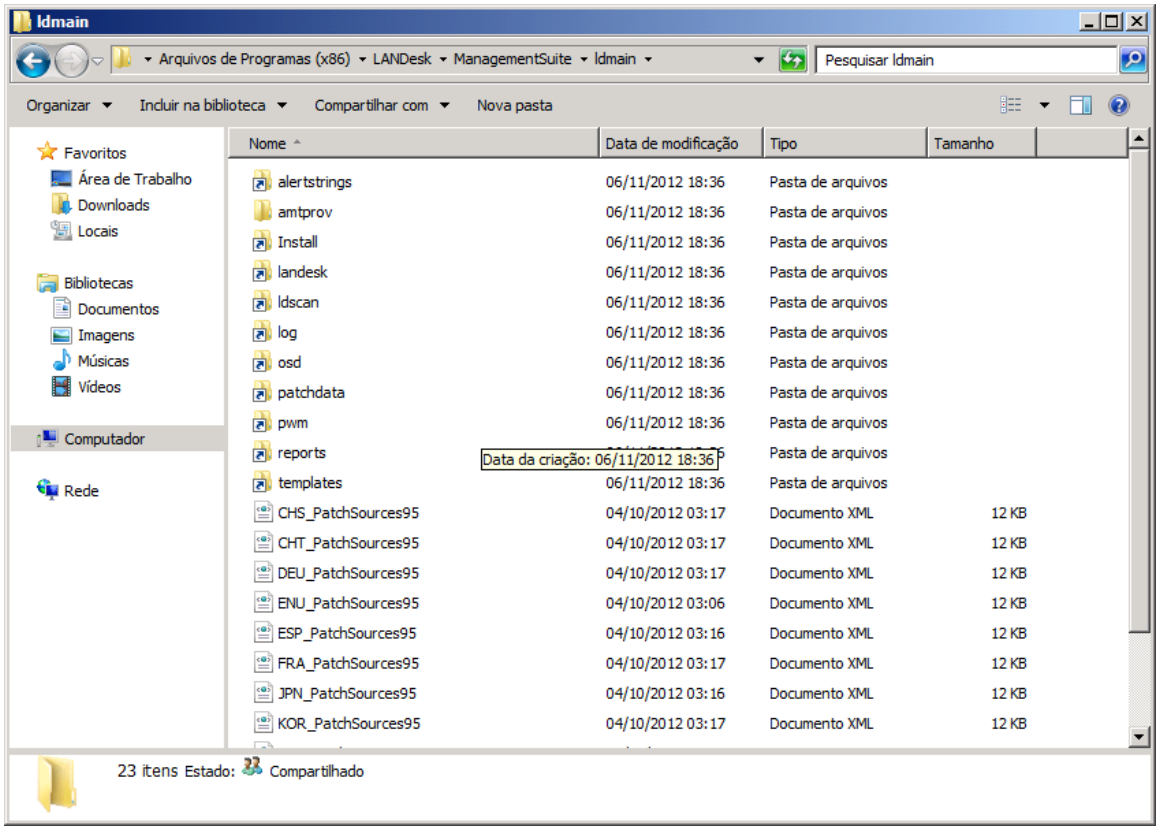
para uma nova subpasta separada chamada:

```
C:\Arquivos de Programas (x86)\LANDesk\ManagementSuite\ldmain (que agora é uma nova pasta distinta)
```

Agora, o compartilhamento LDMAIN contém menos arquivos e pastas. Os administradores (com os direitos apropriados) ainda podem copiar quaisquer arquivos de programa que desejarem para o compartilhamento LDMAIN, que agora tem uma estrutura muito mais limpa, limitada e concentrada.

IMPORTANTE: Os direitos de administração com base em funções foram restritos
Além disso, o direito de administração com base em funções foi restrito a fim de impedir o acesso ao compartilhamento LDMAIN. O grupo da LANDesk Management Suite já não tem os direitos de **Controle total** ou de **Modificação** dessa pasta. Os membros desse grupo ainda podem ler e executar scripts etc. Somente os membros do grupo Administradores da LANDesk têm esses direitos e podem gravar ou editar arquivos no compartilhamento LDMAIN.

A pasta LDMAIN contém diversas subpastas que são simplesmente junções ou indicadores no sistema de arquivos para a pasta real na pasta \LANDesk\ManagementSuite\ldmain. As pastas de junção são identificadas pela sobreposição da seta, conforme exibido abaixo:



Aprimoramentos de segurança dos serviços Web e do console Web

As seguintes alterações foram realizadas no console Web e serviços Web que aumentam a segurança do servidor núcleo LANDesk.

- A segurança de site foi atualizada baseado em prova de penetração (por exemplo, transversal de caminho, cruz-local orquestrando, outras vulnerabilidades sabidos de teia).
- O console de Web foi atualizado a. REDE 4,0.
- A segurança de console de teia completamente foi testada e foi verificado.
- Console não utilizado de Web informando páginas foram retiradas.

NOTA: Mais detalhes sobre mudanças específicas ao console de Web e serviços
de Web Para mais detalhes sobre melhorias de segurança somam ele console de Web e serviços de Web, vêem o documento de BKM localizado na Comunidade de Operador de LANDesk.

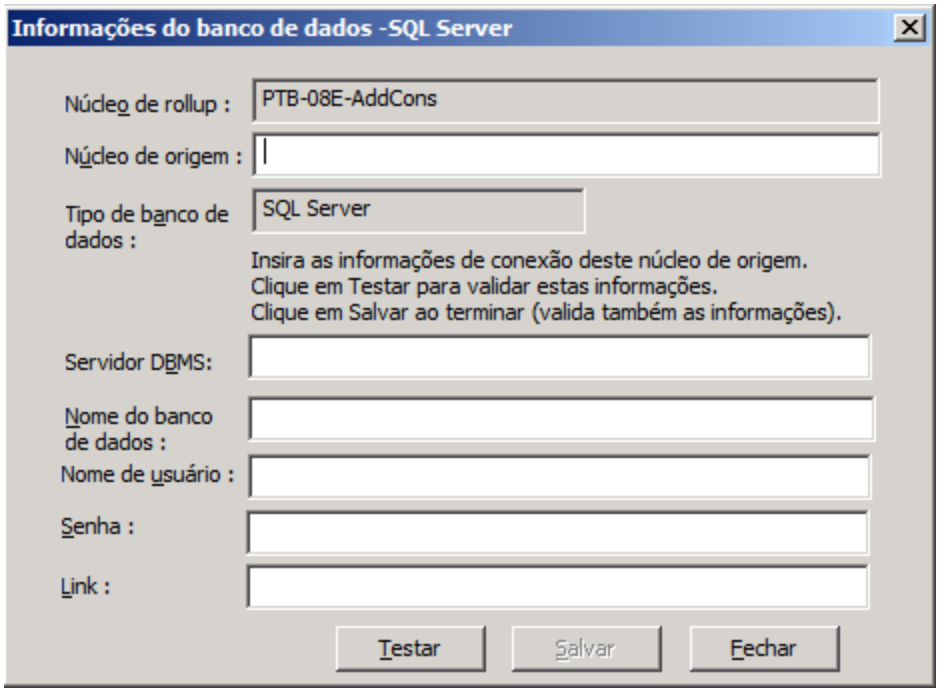
O acesso remoto ao registro está desativado

Acesso remoto de registro ao servidor núcleo foi retirado. Isso foi feito removendo os direitos de leitura/gravação de todos os grupos LANDesk de administração com base em funções. Os direitos de segurança foram removidos do grupo LANDesk Management Suite para a seguinte chave de registro:

```
HKEY_LOCAL_MACHINES\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg
```

Então, agora, em vez de usar registro remoto lê, os usos de console de Controle Remoto seguram Serviços de Web. Estas mudanças devem ser transparentes ao usuário de LANDesk.

Além disso, a interface do usuário do DBRolllup.exe foi atualizada. Agora exige que o administrador entra as informações de configuração de DB. Isto elimina as chamadas remotas de registro entre o servidor núcleo e centro de rollup, como mostrado abaixo:


Informações do banco de dados -SQL Server
Núcleo de rollup :
PTB-08E-AddCons
Núcleo de origem :
Tipo de banco de dados :
SQL Server
Insira as informações de conexão deste núcleo de origem.
Clique em Testar para validar estas informações.
Clique em Salvar ao terminar (valida também as informações).
Servidor DBMS:
Nome do banco de dados :
Nome de usuário :
Senha :
Link :
Testar
Salvar
Fechar

Atualizações do Open SSL

Como o Open SSL evoluiu com o tempo, tornou-se mais seguro. Atualmente, a suporte LANDesk oferece a última versão atualizada do Open SSL.

SSL aberto está agora versão 1.0.1c. Esta versão de SSL Aberto resolveu várias vulnerabilidades sabidos.

Para achar a versão mais recente de SSL Aberto na Comunidade de Operador de LANDesk, vá à página principal em:

Página inicial da Comunidade de usuários da LANDesk

NOTA: De trás para a frente compatibilidade para SSL Aberto foi mantido
LANDesk manteve de trás para a frente compatibilidade com SSL Aberto usando os mesmos algoritmos.

Aprimoramentos do banco de dados criptografados

A coluna CONNECTINFO na tabela metasystems agora está criptografada para que os usuários NÃO possam ler as informações.

Características/itens removidos para aprimorar a segurança do núcleo

As seguintes ferramentas, recursos e componentes foram removidos da versão LANDesk Management Suite do produto 9.5 pois os recursos não foram utilizados nem havia suporte para eles (ou para aprimorar a segurança geral do sistema, reduzindo os serviços associados).

Em outras palavras, os seguintes recursos NÃO estão incluídos no Management Suite ou versões Security Suite9.5 e NÃO devem ser considerados como recursos operacionais ou de suporte:

- Serviço de inventário fora do núcleo.
- Console Web fora do núcleo
- Gerenciador de dispositivos de mão
- Instalação do agente do NetWare
- LinuxPE
- Implantação do servidor NetWare
- Replicador de arquivos obsoletos a partir de utilitários relevantes
- Reparo do aplicativo
- LANDesk Profile Migration

Tópicos relacionados

Visite o site da Comunidade de suporte a usuários da LANDesk para obter mais detalhes sobre as ferramentas removidas e os recursos da versão LANDesk Management Suite9.5:

Página inicial da Comunidade de usuários da LANDesk

Configuração do serviço de núcleo

Configuração de serviços

Muitas das funções integrais e fundamentais fornecidas pelos componentes do LANDesk como servidor de inventário e serviço do planejador podem, e devem ser configuradas para otimizar o desempenho no seu ambiente de rede particular. Faça isso usando o miniaplicativo **Configurar serviços do Software LANDesk**que pode ser iniciado a partir do grupo de programas do menu Iniciar.do **LANDesk** (ou vá em **Configurar > Serviços** em no console de gerenciamento).

NOTA: A configuração de serviços é restrita aos Administradores LANDesk Administrators
Somente um usuário com direito de Administrador da LANDesk pode modificar as configurações do serviço. Além disso, a opção **Configurar serviços** está disponível somente no console principal e não dos consoles adicionais que você tiver configurado.

Este tópico contém informações sobre:

- "Seleção de um banco de dados e um servidor núcleo" na página 80
- "Configuração do serviço de Inventário" na página 81
- "Resolução de registros de dispositivo duplicados no banco de dados" na página 83
- "Configuração do serviço do Agendador" na página 85
- "Configuração do Serviço de trabalhos personalizados" na página 87
- "Configuração do serviço de Multidifusão" na página 88
- "Configuração do serviço de distribuição de SO" na página 88
- "Configuração da senha do BMC" na página 90
- "Configuração de credenciais de virtualização de SO" na página 91

Seleção de um banco de dados e um servidor núcleo

Antes de configurar um serviço, use a guia **Geral** para especificar o servidor núcleo e o banco de dados para os quais o serviço será configurado.

NOTA: qualquer mudança de configuração de serviço feita para um banco de dados e um servidor núcleo não terá efeito até que o serviço seja reiniciado no servidor núcleo.

Sobre a guia Geral

Use esta guia para selecionar o banco de dados e o servidor núcleo para os quais o serviço será configurado. Em seguida, selecione qualquer guia de serviço e especifique as configurações para esse serviço.

As credenciais de usuário do banco de dados de Relatórios permite que a conexão com o banco de dados com uma conta de usuário diferente quando usar a ferramenta Relatórios. Por exemplo, você pode criar um conta de usuário para o banco de dados com ´permissão somente leitura e depois usar esta conta para permitir que usuários de relatórios possam ler o banco de dados, mas não modificá-lo.

- **Nome do servidor:** Exibe o nome do servidor núcleo ao qual você está conectado.
- **Servidor:** permite digitar o nome de um outro servidor núcleo e seu diretório de banco de dados.
- **Banco de dados:** permite digitar o nome do banco de dados núcleo.

- **Nome de usuário:** identifica um usuário com credenciais de autenticação para o banco de dados núcleo (especificadas durante a configuração).
- **Senha:** identifica a senha do usuário necessária para acessar o banco de dados núcleo (especificada durante a configuração).
- **Este é um banco de dados Oracle:** indica que o banco de dados núcleo especificado é um banco de dados Oracle.
- **Usuário do banco de dados Relatórios:** Especificar o nome de usuário e senha da conta que você quer que seja usada na ferramenta Relatórios para acessar o banco de dados. Essa conta já deverá ter sido criada com permissões específicas de acesso ao banco de dados.
- **Configurações do Web Console:** Mostra o nome do servidor ou o endereço IP no qual o Web console pode ser executado. Quando você quiser acessar o Web console de outro dispositivo, você digita este nome ou endereço, seguido de /remote, em um navegador de web.
- **Atualizar configurações:** Restaura as configurações que estavam em vigor quando a caixa de diálogo foi aberta.

Ao especificar nomes de usuário e senhas para um banco de dados, eles não podem conter apóstrofe ('), ponto e vírgula (;) ou o sinal de igual (=).

Configuração do serviço de Inventário

Use a guia **Inventário** para configurar o Serviço de inventário para o servidor núcleo e o banco de dados selecionados com a guia Geral.

Se você precisar reiniciar o serviço de Inventário em um núcleo em cluster, você precisará fazer isso através do Gerenciador de controle de serviço Windows. O botão **Reiniciar** serviços na guia **Inventário** do LANDesk Software Services não pode reiniciar o serviço Inventário em um núcleo em cluster.

Sobre a guia Inventário

Use essa guia para especificar as seguintes opções de inventário:

- **Nome do servidor:** Exibe o nome do servidor núcleo ao qual você está conectado.
- **Estatísticas de log:** mantém um log de ações e estatísticas do banco de dados núcleo. Você pode ver os dados no log do Aplicativo do Visualizador de evento do Windows.
- **Dados criptografados de transporte:** permite que a análise de inventário envie dados de inventário do dispositivo analisado de volta para o servidor núcleo como dados criptografados através de SSL.
- **Analisar servidor em:** especifica a hora em que o servidor núcleo será analisado.
- **Realizar manutenção em:** especifica a hora da manutenção padrão do banco de dados núcleo.
- **Dias para guardar as análises de inventário:** Define o número de dias antes que o registro de análise do inventário seja excluído.
- **Logins do proprietário principal:** define o número de vezes em que o analisador de inventário acompanhará os inícios de sessão para determinar o proprietário principal de um dispositivo. O proprietário principal é o usuário que iniciou mais sessões dentro deste número específico de inícios de sessão. O valor padrão é 5 e os valores mínimo e máximo são 1 e 16, respectivamente. Se cada início de sessão for diferente do anterior, o último usuário a iniciar uma sessão será considerado o proprietário principal. Um dispositivo pode ter apenas um proprietário principal associado a ele por vez. Os dados de início de sessão do usuário principal incluem o nome totalmente qualificado do usuário no formato ADS, NDS, nome de domínio ou nome local (nessa ordem), além da data do último início de sessão.

- **Configurações avançadas:** Exibe a caixa de diálogo **Configurações avançadas**. As configurações avançadas relacionadas ao inventário podem ser mudadas aqui. Ao clicar em cada item, aparece o texto de ajuda na base do diálogo que explica cada opção. Os valores padrões devem ser o suficiente para a maioria das instalações. Para mudar uma configuração, clique nela, mude o **Valor**, em seguida, clique em **Definir**. Reinicie o serviço de inventário quando terminar.
- **Itens desconhecido:** Abre a caixa de diálogo **Itens de inventário desconhecidos**, que contém qualquer objeto que foi encontrado em análises e que ainda não está no banco de dados. Isso dá a você controle sobre que novos itens são adicionados ao banco de dados para que você possa eliminar problemas potenciais com os dados. Você pode escolher permitir aos dados serem adicionados ao banco de dados, é só excluir os dados desta lista ou ignorar o item em todas as análises futuras.
- **Software:** Exibe a caixa de diálogo **Configurações de análise de software**. Define o horário de execução das análises de software e por quanto tempo salvar o histórico do inventário.
- **Atributos:** Abre a caixa de diálogo **Selecionar os atributos a serem armazenados** onde é possível selecionar os atributos de análise de inventário armazenados no banco de dados. Isto pode reduzir o tamanho do banco de dados e aumentar a velocidade de análise.
- **Gerenciar duplicados: Dispositivos**: Abre a caixa de diálogo **Dispositivos duplicados**, onde é possível configurar como os dispositivos duplicados são tratados.
- **Gerenciar duplicados: dispositivos:** Abre a caixa de diálogo **ID de dispositivo duplicado** na qual é possível selecionar atributos que identificam exclusivamente os dispositivos. Você pode usar essa opção para evitar a necessidade de duplicar IDs de dispositivos analisados no banco de dados núcleo (consulte "Resolução de registros de dispositivo duplicados no banco de dados" na página 83).
- **Status do serviço de inventário:** Indica se o serviço foi iniciado ou interrompido no servidor núcleo.
    - **Iniciar:** inicia o serviço no servidor núcleo.
    - **Parar:** interrompe o serviço no servidor núcleo.
    - **Reiniciar:** reinicia o serviço no servidor núcleo.

Sobre o diálogo Itens de inventário desconhecido

A caixa de diálogo **Itens de inventário desconhecidos (botão Itens desconhecidos em Configurar > Serviços > guia Inventário)** permite que você controle quais novos itens serão adicionados ao banco de dados do inventário. Quando a análise de inventário é executada ela pode encontrar objetos que não são identificados no banco de dados. Pode haver dados corrompidos ou outros problemas em um dispositivo gerenciado, por esse motivo você pode precisar evitar colocar novos dados no banco de dados. Esta caixa de diálogo contém todos os itens que foram encontrados e dá a você a opção de adicionar os novos itens ao banco de dados, excluí-los ou bloqueá-los para impedi-los de serem adicionados ao banco de dados.

- **Bloquear itens de inventário desconhecidos:** Quando esta caixa é selecionada, todos os itens desconhecidos são relacionados aqui até você escolher como se dispor deles.
- **Itens bloqueados:** Contém todos os objetos do inventário que não estão atualmente no banco de dados. Clique em um ou mais itens para selecioná-los e aplicar uma ação.
- **Permitir:** Selecione itens e clique em **Permitir** para adicionar os dados ao banco de dados. Os itens serão adicionados aos bancos de dados e isso permite a eles serem processados em futuras análises de inventário.
- **Excluir:** Selecione itens e clique em **Excluir** para removê-los desta lista apenas. Se o item for encontrado novamente, ele será relacionado novamente. Tipicamente você excluiria itens que são resultado de corrupção de dados e nunca serão encontrados novamente em uma análise.

- **Ignorar:** Selecione itens e clique em **Ignorar** para bloqueá-los permanentemente para não serem adicionados ao banco de dados. Por razões de desempenho, a lista Ignorar deve ser mantida o mais curta possível. Note que os itens nessa lista são ignorados permanentemente; a única maneira de removê-los da lista a de removê-los manualmente da tabela META_IGNORE do banco de dados do inventário e reiniciar o serviço de inventário.
- **OK/Cancelar:** Nessa caixa de diálogo os botões **OK** e **Cancelar** aplicam-se apenas à caixa de seleção **Bloquear itens de inventário desconhecidos** e não a qualquer ação nos itens bloqueados.

Sobre o diálogo Configurações de análise de software.

Use esta caixa de diálogo (**Configurar > Serviços > guia Inventário > botão Software)** para configurar a frequência das análises de software. O hardware de um dispositivo é analisado sempre que é executada a análise de inventário no dispositivo, mas o software do dispositivo é analisado somente no intervalo especificado aqui.

- **A cada login:** Analisa todos os software instalados no dispositivo cada vez que o usuário faz o login.
- **Uma vez a cada (dias):** faz a análise do software do dispositivo somente no intervalo de dias especificado, como uma análise automática.
- **Salvar histórico (dias):** especifica o tempo durante o qual o histórico de inventário do dispositivo ficará gravado. Limpar a caixa de seleção não salva o histórico de inventário.

Configuração para determinar que atributos de análise de invetário são armazenados no banco de dados

O analisador de inventário procura centenas de itens de inventário. Se não precisar de todas essas informações de análise no banco de dados, você pode limitar o número de atributos de análise a ser armazenado no banco de dados, acelerar o tempo de inserção de análise e reduzir o tamanho do banco de dados. Quando isso é feito, os dispositivos gerenciados ainda submetem análises de inventário completas, mas o serviço de inventário do núcleo só armazena os atributos que forem especificados no banco de dados.

Como padrão, o serviço de inventário insere todos os atributos de análise no banco de dados. As mudanças de filtro de atributo que fizer não afetarão os dados já armazenados no banco de dados. Para limitar os dados que são armazenados, siga as etapas abaixo.

Para configurar filtragem de dados de análise de inventário

1. Clique na guia **Configurar > Serviços > Inventário** botão **> Atributos**.
2. Os atributos na coluna **Atributos selecionados** à direita são inseridos no banco de dados. Transfira os atributos que não quiser armazenar no banco de dados para a coluna **Atributos disponíveis**. Ao terminar, clique em **OK**.
3. Reinicie o serviço de inventário clicando em **Reiniciar** na guia Inventário.
4. Clique em **OK**.

Resolução de registros de dispositivo duplicados no banco de dados

Em alguns ambientes são usadas imagens de SO de maneira regular e freqüente para configurar dispositivos. Por essa razão, a possibilidade de duplicar IDs de dispositivos aumenta. Esse problema pode ser evitado especificando outros atributos exclusivos de dispositivos que, combinados com o ID do dispositivo, criam um identificador exclusivo para os dispositivos. Exemplos desses outros atributos são o nome do dispositivo, o nome do domínio, BIOS, barramento, co-processador, etc.

O recurso de ID duplicado permite selecionar atributos de dispositivos que possam ser usados para identificar exclusivamente o dispositivo. Especifique quais são esses outros atributos e quantos deles devem estar ausentes antes de o dispositivo ser designado como uma duplicação de um outro dispositivo. Se o analisador de inventário não puder detectar um dispositivo duplicado, ela gravará um evento no log de eventos de aplicativos para indicar o ID do dispositivo duplicado.

Além de IDs de dispositivos duplicados pode também haver nomes de dispositivos ou endereços MAC duplicados que foram acumulados no banco de dados. Se ocorrer problemas de dispositivos duplicados constantemente (e quiser impedir futuros registros de dispositivos duplicados por análises e incluídos no seu banco de dados), você pode também especificar que sejam removidos quaisquer nomes de dispositivo duplicados residentes atualmente no banco de dados. Esse recurso que trata de dispositivos duplicados suplementares está incluído no procedimento abaixo.

Para configurar o tratamento de dispositivos duplicados

1. Clique em **Configurar > Serviços > Inventário > IDs de dispositivo**.
2. Selecione os atributos na lista **Lista de atributos** que deseja usar para identificar exclusivamente um dispositivo e, em seguida, clique no botão **>>** para adicionar o atributo à lista **Atributos de identidade**. Você pode adicionar quantos atributos desejar.
3. Selecione o número de atributos de identidade (e atributos de hardware) que um dispositivo não deve encontrar antes de ser considerado uma duplicação de outro dispositivo.
4. Se desejar que o analisador de inventário rejeite os IDs de dispositivos duplicados, selecione a caixa de seleção **Rejeitar identidades duplicadas**.
5. Clique em **OK** para salvar suas configurações e voltar para a caixa de diálogo **Configurar inventário**.
6. (Opcional) Se quiser também resolver dispositivos duplicados por nome e/ou endereço clique em **Dispositivos** para abrir a caixa de diálogo **Dispositivos duplicados** onde você pode especificar as condições em que os dispositivos duplicados são removidos, por exemplo, quando os nomes de dispositivo correspondem, endereços MAC correspondem ou ambos correspondem.

Sobre a caixa de diálogo ID de dispositivo duplicado

Use esta caixa de diálogo (clique em **Configurar > Serviços > guia Inventário > botão IDs de dispositivos)** para configurar a forma como o ID do dispositivo duplicado deve ser tratado.

- **Lista de atributos:** contém todos os atributos que podem ser selecionados para identificar exclusivamente um dispositivo.
- **Atributos de identidade:** mostra os atributos selecionados para identificar exclusivamente um dispositivo.
- **Acessar como ID de dispositivo duplicado quando:** identifica o número de atributos que um dispositivo não deve encontrar antes de ser considerado uma duplicação de outro dispositivo.
- **Rejeitar identidades duplicadas:** Faz com que o analisador de inventário registre o ID do dispositivo duplicado e rejeite todas as tentativas subseqüentes de analisar esse ID de dispositivo. Em seguida, o analisador de inventário gera um novo ID de dispositivo.

Sobre a caixa de diálogo Propriedades do dispositivo

Use este diálogo (clique em **Configurar > Serviços > Inventário** botão **> Dispositivos**) para especificar o nome e/ou as condições de endereço quando dispositivos duplicados forem removidos do banco de dados. Quando uma das opções de remoção de duplicados é selecionada, os duplicados são permitidos no banco de dados, mas serão removidos a próxima vez que ocorrer a manutenção no banco de dados.

- **Remover duplicado quando:**
  - **Os nomes dos dispositivos coincidem:** remove o registro antigo quando dois ou mais nomes de dispositivos corresponderem no banco de dados.
  - **Os endereços MAC coincidem:** Remove o registro antigo quando dois ou mais endereços MAC corresponderem no banco de dados.
  - **Os nomes dos dispositivos e os endereços MAC coincidem:** Remove o registro antigo somente quando dois ou mais nomes e endereços MAC de dispositivos correspondem (no mesmo registro).
- **Restaurar IDs de dispositivos antigos:** Restaura o ID original do dispositivo do registro mais antigo de um dispositivo analisado, *se* existirem dois registros do dispositivo no banco de dados e pelo menos uma das opções de remoção acima for selecionada e seus critérios forem satisfeitos. O ID original do dispositivo é restaurado quando a próxima análise de manutenção de inventá for executada. Esta opção não tem efeito a menos que uma das opções de remoção acima seja selecionada.

Configuração do serviço do Agendador

Use a guia **Agendador** para configurar o Serviço do agendador (**Ferramentas > Distribuição > Tarefas agendadas**) para o banco de dados e o servidor núcleo selecionado com a guia **Geral**.

Você deve ter os direitos apropriados para executar essas tarefas, incluindo privilégios plenos de administrador para dispositivos Windows na rede, permitindo que eles recebam distribuições de pacotes do servidor núcleo. Você pode especificar credenciais múltiplas de login para usar nos dispositivos clicando em **Alterar login**.

Uma definição adicional que você pode configurar manualmente é a taxa de atualização das **Tarefas agendadas**. Como padrão, a janela **Tarefas agendadas** verifica o banco de dados núcleo a cada dois minutos para determinar se algum dos itens visíveis foi atualizado. Se quiser mudar a taxa de atualização, navegue até a seguinte chave no registro:

- HKEY_CURRENT_USER\Software\LANDesk\ManagementSuite\WinConsole

Defina "TaskRefreshIntervalSeconds" como o número de segundos entre atualizações para uma tarefa ativa. Defina "TaskAutoRefreshIntervalSeconds" como o intervalo de atualização para a janela **Tarefas agendadas** inteira.

Sobre a guia Agendador

Use essa guia para ver o nome do banco de dados e do servidor núcleo selecionado anteriormente e para especificar as seguintes opções de Tarefas agendadas:

- **Nome de usuário:** O nome do usuário no qual o serviço de tarefas agendadas será executado. Essa definição pode ser alterada clicando no botão **Alterar login**.
- **Número de segundos entre as novas tentativas:** quando uma tarefa agendada é configurada com várias novas tentativas, essa configuração controla o número de segundos que o serviço Tarefas agendadas irá aguardar antes de tentar executar a tarefa novamente.
- **Número de segundos para tentar ativar:** Quando uma tarefa agendada é configurada para usar Wake On LAN, essa configuração controla o número de segundos que o serviço Tarefas agendadas irá aguardar pela ativação de um dispositivo.
- **Intervalo entre as avaliações da consulta:** um número que indica o tempo entre as avaliações de consultas e uma unidade de medida para o número (minutos, horas, dias ou semanas).

- **Configurações de Wake on LAN:** a porta IP que será usada pelo conjunto de pacotes Wake On LAN para que o serviço Tarefas agendadas ative os clientes.
- **Status do serviço de agendador:** indica se o serviço de agendador está iniciado ou interrompido no servidor núcleo.
    - **Iniciar:** inicia o serviço no servidor núcleo.
    - **Parar:** interrompe o serviço no servidor núcleo.
    - **Reiniciar:** reinicia o serviço no servidor núcleo.
- **Avançada:** Exibe a caixa de diálogo **Configurações avançadas do agendador**. As configurações relacionadas à agenda podem ser alteradas aqui. Ao clicar em cada item, aparece o texto de ajuda na base do diálogo que explica cada opção. Os valores padrões devem ser o suficiente para a maioria das instalações. Para modificar uma configuração, clique na mesma, clique em **Editar**, digite um novo valor e clique em **OK**. Reinicie o serviço de agendador quando terminar.

Sobre a caixa de diálogo Alterar login

Use a caixa de diálogo **Alterar login** (em **Configurar > Serviços >** guia **Agendador**) para mudar o login padrão do agendador. Você também pode especificar credenciais alternativas que o serviço do planejador deve tentar quando precisar executar uma tarefa em dispositivos não gerenciados.

Para instalar os agentes LANDesk em dispositivos não gerenciados, o serviço do planejador precisa poder conectar-se aos dispositivos com uma conta administrativa. A conta padrão que o serviço do planejador utiliza é LocalSystem. As credenciais LocalSystem geralmente funcionam com dispositivos que não estão em um domínio. Se os dispositivos estão em um domínio, é necessário especificar um conta de administrador de domínio.

Se desejar mudar as credenciais de login do serviço do planejador, você pode especificar uma conta administrativa a nível de domínio diferente para usar nos dispositivos. Se estiver gerenciando dispositivos em vários domínios, adicione credenciais adicionais para o serviço do planejador tentar. Se desejar usar uma conta diferente da LocalSystem para o serviço do planejador ou se desejar fornecer credenciais alternativas, é necessário especificar um login de serviço do planejador primário que tenha direitos administrativos no servidor núcleo. As credenciais alternativas não requerem direitos administrativos no servidor núcleo, mas devem ter direitos administrativos nos dispositivos.

O serviço do planejador experimentará as credenciais padrão e, em seguida, usará cada credencial que você especificou na lista **Credenciais alternativas** até conseguir ou as credenciais terminarem. As credenciais que você especificar são criptografadas com segurança e armazenadas no registro do servidor núcleo.

NOTA: Os servidores de núcleo de rollup usam as credenciais de serviço do agendador para autenticar para fazer a sincronização. Nos núcleos de rollup essas credenciais de serviço do agendador precisam ser membros de um grupo com privilégios de administrador do console nos servidores núcleos de origem. Se as credenciais não tiverem esses privilégios, o rollup falhará e você verá erros no handler de tarefa no log de sincronização do núcleo de origem.

Você pode definir as seguintes opções para as credenciais do agendador padrão:

- **Nome de usuário:** Digite o domínio\nome de usuário padrão ou o nome do usuário que desejar que o agendador use.
- **Senha:** digite a senha do usuário especificado.
- **Confirmar senha:** digite a senha novamente para confirmá-la.

Você pode definir as seguintes opções para as credenciais adicionais do agendador:

- **Adicionar:** Clique para adicionar um novo nome de usuário e senha para a lista de **Credenciais alternativas**.
- **Remover:** clique para remover as credenciais selecionadas da lista.
- **Modificar:** clique para mudar as credenciais selecionadas.

Ao adicionar credenciais alternativas, especifique o seguinte:

- **Nome de usuário:** Digite o nome de usuário que desejar que o Agendador use.
- **Domínio:** Digite a senha do usuário especificado.
- **Senha:** digite a senha para as credenciais que especificou.
- **Confirmar senha:** digite a senha novamente para confirmá-la.

Configuração do Serviço de trabalhos personalizados

Use a guia **Trabalhos personalizados** para configurar o serviço de trabalhos personalizados para o servidor núcleo e o banco de dados selecionados na guia Geral. Exemplos de trabalhos personalizados incluem análises de inventário, distribuição de dispositivos ou distribuições de software.

Os trabalhos podem ser executados com um dos dois protocolos remotos, TCP ou o protocolo de agente LANDesk padrão, CBA. Quando o TCP é desabilitado como o protocolo de execução remota, o serviço Trabalhos personalizados usa o protocolo agente LANDesk padrão, por padrão, esteja ele marcado ou não como desabilitado. Além disso, se ambos os protocolos de execução remota TCP e agente LANDesk padrão forem habilitados, o serviço de tarefas personalizadas tenta usar primeiro o protocolo TCP de execução remota e, se este não estiver disponível, será usada a execução remota do agente LANDesk padrão.

Os **Trabalhos personalizados** também o habilitam a escolher opções para a descoberta de dispositivos. Antes do serviço trabalhos personalizados poder processar um trabalho, ele precisa descobrir o endereço IP de cada dispositivo. Esta guia permite configurar a forma como o serviço contata os dispositivos.

Sobre a caixa de diálogo Configurar serviços da LANDesk Software: Guia Trabalhos personalizados

Use essa guia para definir as seguintes opções de Trabalhos personalizados:

Opções de execução remota

- **Desabilitar execução de TCP:** Desativa o TCP como protocolo de execução remota utilizando, conseqüentemente, o protocolo agente LANDesk padrão como padrão.
- **Desabilitar execução/transferência de arquivos via CBA:** Desabilita o agente LANDesk padrão como o protocolo de execução remota. Se o agente LANDesk padrão for desabilitado e o protocolo TCP de execução remota não for localizado no dispositivo, a execução remota não ocorrerá.
- **Habilitar o tempo limite de execução remota:** habilita um tempo limite de execução remota e especifica o número de segundos após os quais o tempo limite irá ocorrer. Os tempos limites de execução remota são ativados quando o dispositivo envia pulsações, mas o trabalho no dispositivo está suspenso ou em loop. Esta configuração aplica-se aos dois protocolos (TCP ou agente LANDesk padrão). Esse valor pode variar entre 300 segundos (5 minutos) e 86.400 segundos (1 dia).
- **Habilitar o tempo limite de um cliente:** habilita o tempo limite de um dispositivo e especifica o número de segundos após os quais o tempo limite irá ocorrer. Por padrão, o TCP de execução remota envia um pacote do dispositivo para o servidor em intervalos de 45 segundos até que a execução remota seja concluída ou o seu tempo limite seja atingido. Os tempos limites de dispositivos são ativados quando o dispositivo não envia uma pulsação ao dispositivo.
- **Porta de execução remota:** especifica a porta pela qual ocorre o TCP de execução remota. O padrão é 12174. Se essa porta for mudada, ela também deverá ser mudada na configuração do dispositivo.

Opções de distribuição

- **Distribuir para <nn> computadores simultaneamente:** Especifica o número máximo de dispositivos aos quais o trabalho personalizado será distribuído simultaneamente.

Opções de descoberta

- **UDP:** Selecione UDP para usar ping de agente LANDesk via UDP. A maioria dos componentes de dispositivos LANDesk depende do agente LANDesk padrão, portanto, seus dispositivos gerenciados devem ter o agente LANDesk padrão instalado. Este é o método de descoberta mais rápido e o padrão. Com o UDP, você pode também selecionar o número de ping UDP de **Tentativas** e um valor de **Tempo limite**.
- **TCP:** A seleção de TCP usa uma conexão HTTP para o dispositivo na porta 9595. Esse método de descoberta oferece o benefício de ser capaz de funcionar através de uma firewall se você abrir a porta 9595, mas está sujeito a tempos limites de conexão de HTTP se os dispositivos não estiverem presentes. Esses tempos limite podem durar 20 segundos ou mais. Se um grupo de dispositivos alvo não responder à conexão TCP, a sua tarefa levará algum tempo para começar.
- **Ambos:** Selecione Ambos faz o serviço tentar a descoberta com UDP primeiro, com TCP e, por último, com DNS/WINS, se selecionado.
- **Desabilitar transmissão de sub-rede:** Quando selecionada, esta opção desabilita a descoberta via difusão de sub-rede. Quando selecionada, esta opção resultará em uma transmissão direcionada a uma sub-rede sendo enviada através de UDP usando PDS.
- **Desabilitar procura de DNS/WINS** quando selecionada, esta opção desabilita uma pesquisa de serviço de nomes para cada dispositivo se o método de descoberta TCP/UDP falhar.

Configuração do serviço de Multidifusão

Use a guia **Multidifusão** para configurar as opções de descoberta do representante do domínio multidifusão para o banco de dados e para o servidor núcleo selecionado com a guia Geral.

Sobre a guia Multidifusão

Use essa guia para definir as seguintes opções de multidifusão:

- **Usar o representante de domínio de multidifusão:** utiliza a lista de representantes de domínio de multidifusão armazenados no grupo **Configuração > Representantes de domínio de multidifusão** na tela da rede.
- **Usar arquivo em cache:** pesquisa cada domínio de multidifusão para descobrir quem já possui o arquivo, eliminando, portanto, a necessidade de fazer o download do arquivo para um representante.
- **Usar arquivo em cache antes do representante do domínio preferido:** muda a ordem da descoberta para que **Usar arquivo em cache** seja a primeira opção a ser utilizada.
- **Usar transmissão:** envia uma transmissão direcionada a sub-rede para localizar qualquer dispositivo nessa sub-rede que possa ser um representante de domínio de multidifusão.
- **Período de descarte de log:** especifica o número de dias que as entradas no log serão retidas antes de serem excluídas.

Configuração do serviço de distribuição de SO

Use a guia **Distribuição de SO** para designar representantes de PXE como filas de espera PXE e para configurar as opções básicas de inicialização de PXE para o banco de dados e para o servidor núcleo selecionado na guia Geral.

As filas de espera PXE são um método de distribuir imagens de SO para dispositivos habilitados no PXE. Atribua os representantes de PXE existentes (localizados no grupo **Configuração** da tela de rede) como filas de espera PXE. Para obter mais informações, consulte "Visão geral do Distribuição baseada no PXE" na página 368.

Selecione e mova os representantes de PXE da lista **Proxies disponíveis** para a lista de **Proxies da fila de espera**.

Sobre a guia Distribuição de SO

Use essa guia para atribuir proxies (representantes) de filas de espera PXE e para especificar as opções de inicialização de PXE.

- **Proxies disponíveis:** mostra todos os proxies do PXE disponíveis na rede, identificados pelo nome do dispositivo. Essa lista é gerada quando o analisador de inventário detecta o software do PXE (PXE) e os protocolos MTFTP em execução no dispositivo.
- **Proxies da fila de retenção:** mostra os proxies de PXE que foram movidos da lista **Proxies disponíveis**, designando assim o proxy como uma fila de espera PXE. Os dispositivos habilitados para PXE na mesma sub-rede que o proxy de fila de espera PXE serão automaticamente adicionados ao grupo **Fila de espera PXE** na tela de rede do console quando inicializarem o PXE. Os dispositivos poderão ser agendados para uma tarefa de distribuição de imagem.
- **Redefinir:** força todos os dispositivos habilitados no PXE na mesma sub-rede como o representante de PXE selecionado a entrar novamente na **Fila de espera PXE** na tela de rede do console. Os dispositivos podem então ser agendados para uma tarefa de criação de imagem. (O botão Redefinir será ativado quando você selecionar um proxy PXE na lista de Proxies da fila de espera).

NOTA: As mudanças feitas aqui para as opções de inicialização do PXE não terão efeito em nenhum dos representantes de PXE até que o script Distribuição de representante de PXE seja executado nesse representante.

- **Tempo limite:** indica quanto tempo o prompt de inicialização é mostrado antes de ser atingido o tempo limite e de continuar com o processo padrão de inicialização. O número máximo de segundos é 60 segundos.
- **Mensagem:** especifica a mensagem no prompt de inicialização de PXE exibida no dispositivo. Você pode digitar qualquer mensagem que desejar na caixa de texto com um tamanho máximo de 75 caracteres.

Validação do seu ambiente de pré-inicialização da distribuição do SO

Clique no botão **Validação de OSD** para abrir a caixa de diálogo **Ambiente de imagem de OSD**, com o qual você pode validar sua licença para usar um ambiente de pré-inicialização em DOS ou Windows para distribuição do SO.

Sobre a caixa de diálogo do ambiente de imagem de OSD

Use a caixa de diálogo **Ambiente de imagem OSD** para validar a sua licença para usar um ambiente de pré-inicialização em DOS ou Windows. Os requisitos de validação de licença são os seguintes:

- **Windows PE:** Ao clicar no botão Licença, as informações sobre a licença Windows PE incluída neste produto são exibidas. Você deve aceitar os termos da licença antes de usar o Windows PE com distribuição ou provisionamento de OS.
- **DOS:** A verificação da licença exige o CD de servidor Windows NT 4 e o CD Windows 98.

Para validar um ambiente DOS PE

1. Clique no botão **Validação de OSD** na guia **Distribuição de SO**. (Se você estiver usando a ferramenta de distribuição de SO, clique no botão **Validar licenças** na barra de tarefas.)
2. Na seção **Ambiente de imagem DOS** clique em **Validar agora**.
3. Insira um CD de instalação de servidor Windows NT4 em uma unidade. Clique em **Procurar** e selecione a pasta \CLIENTS\MSCLIENT\DISKS no CD.
4. Clique em **OK**. O processo de validação acessa arquivos nesse CD. Quando terminar, ele avisa para colocar o próximo CD.
5. As ser solicitado, insira um CD de instalação do Windows 98 em uma unidade. Clique em **Procurar** e selecione a pasta \WIN98 no CD.
6. Clique em **OK**. O processo de validação continuará e quando terminar, clique em **OK**.

Para aceitar a licença para o Ambiente do Windows PE

1. Clique no botão **Validação de OSD** na guia **Distribuição de SO**. (Se você estiver usando a ferramenta de distribuição de SO, clique no botão **Validar licenças** na barra de tarefas.)
2. Na seção **Contrato de licença do Windows PE**, clique em **Licença**.
3. Clique no link para aceitar os termos da licença WAIK. A mensagem "Aceito" é exibida na caixa de diálogo Ambiente de imagem OSD.

IMPORTANTE: Este produto instala componentes do Windows Automated Installation Kit (WAIK) para Windows 7 como parte da instalação do produto, que inclui um Ambiente do Windows PE. Não instale qualquer outra versão do WAIK no servidor núcleo ou haverá conflitos entre as duas versões do WAIK. Se você quiser usar qualquer outra versão do WAIK, instale-o em outro dispositivo, diferente do servidor núcleo.

Para selecionar um ambiente de pré-inicialização padrão

1. Após ter validado os ambientes de pré-inicialização que deseja usar, volte para a caixa de diálogo Ambiente de imagem OSD.
2. Na lista **Ambiente de pré-inicialização padrão**, selecione **Linux** ou **Windows** como seu ambiente de pré-inicialização padrão.
3. Clique em **OK**.

Configuração da senha do BMC

Use a guia **Senha BMC** para criar uma senha para o BMC (Baseboard Management Controller) IPMI nos dispositivos habilitados com IPMI.

- **Senha:** Digite a senha a ser usada para BMC nos dispositivos IPMI.
- **Confirmar senha:** Digite outra vez a senha na caixa de texto, em seguida clique em **Aplicar** ou em **OK** para configurar a senha.

A senha não pode ser maior que 15 caracteres e só pode conter números de 0 a 9 ou as letras de a a z maiúsculas ou minúsculas.

Configuração de credenciais de virtualização de SO

Use a guia **Virtualização de SO** para digitar credenciais para gerenciar servidores VMware ESX que são configurados como hosts de SO virtual. Os hosts de SO virtual que foram descobertos são mostrados na tela de rede em uma pasta separada **Hosts de SO Virtual**.

- **Nome de usuário:** Digite o nome de usuário padrão.
- **Senha e Confirmar senha:** Digite e confirme a senha a ser usada, em seguida, clique em **Aplicar** ou em **OK** para configurar as credenciais.

Sincronização do núcleo

Sincronização do núcleo

A sincronização de núcleo permite que você pode copie configurações e tarefas entre núcleos, manualmente ou automaticamente. É possível usar este recurso para manter múltiplos núcleos sincronizados com um núcleo master.

Você pode sincronizar os seguintes itens:

- Configurações de agente
- Alertas
- Configurações de coluna
- Métodos de entrega
- Pacotes de distribuição
- Configurações de gerenciamento de energia
- Pesquisas e configurações de coluna de pesquisa
- Scripts
- Configuração de agente (**NOTA:** Anteriormente conhecido como Configurações de Patch e Segurança)
- Tarefas e normas

Há três meios para sincronizar itens:

- Por demanda
- Automaticamente
- Importar/Exportar

Ao exportar/sincronizar tarefas ou configurações de pacote de distribuição de software, os dados de exportação/sincronização conterão pesquisas associadas e itens relacionados. Observe que os dados de exportação/sincronização contêm informações do banco de dados do Management Suite. Por exemplo, arquivos de exportação de distribuição de software não conterão o verdadeiro pacote sendo distribuído.

Com relação a isso, ao trabalhar com tarefas agendadas de exportação/sincronização, certifique-se de que os caminhos de pacotes sejam os mesmos dos servidores fonte e alvo. Caso contrário, quando você importar/sincronizar a tarefa e executá-la, ela falhará porque o servidor alvo não conseguirá encontrar o pacote.

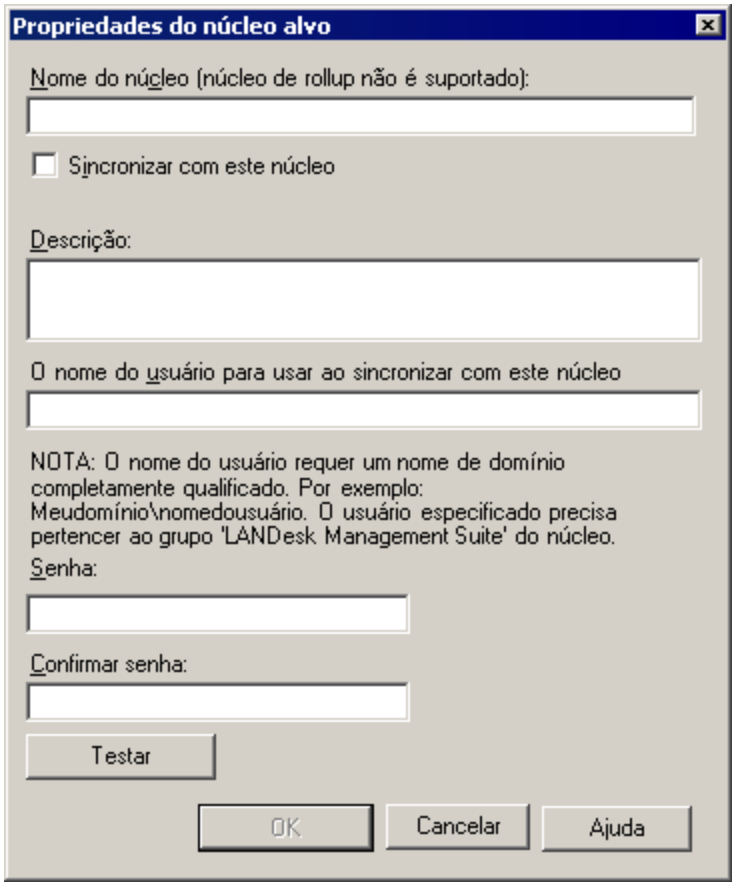
Quando você copiar ou autosincronizar um item, o seguinte acontece:

1. O servidor fonte núcleo cria um arquivo de exportação .ldms XML contendo as informações necessárias para recriar o item alvo e quaisquer itens referenciados pelo item alvo.
2. O servidor alvo núcleo conecta através do HTTPS ao serviço Web de segurança do servidor fonte núcleo e transmite o arquivo .ldms.
3. O serviço Web de segurança do núcleo alvo copia o arquivo .ldms recebido à pasta C:\Arquivos de programa\LANDesk\ManagementSuite\exportablequeue.
4. O serviço de sincronização núcleo verifica esta pasta regularmente para ver novos arquivos. Ele encontra o arquivo exportado a partir do núcleo fonte e o importa, removendo-o da pasta.

NOTA: A distribuição do SO e as ferramentas de monitoração de licença de software não suportam sincronização do núcleo.

Adicionar servidores à lista de sincronização de núcleo

Antes de poder usar a sincronização, é necessário configurar a lista de servidores com as quais você quer sincronizar. Os núcleos comunicam-se através do HTTPS e autenticam-se com um nome de usuário e senha fornecidos por você, para cada núcleo.


Propriedades do núcleo alvo
Nome do núcleo (núcleo de rollup não é suportado):
Sincronizar com este núcleo
Descrição:
O nome do usuário para usar ao sincronizar com este núcleo
NOTA: O nome do usuário requer um nome de domínio completamente qualificado. Por exemplo: Meudomínio\nomedousuário. O usuário especificado precisa pertencer ao grupo 'LANDesk Management Suite' do núcleo.
Senha:
Confirmar senha:
Testar
OK
Cancelar
Ajuda

Para adicionar um servidor núcleo à lista de sincronização

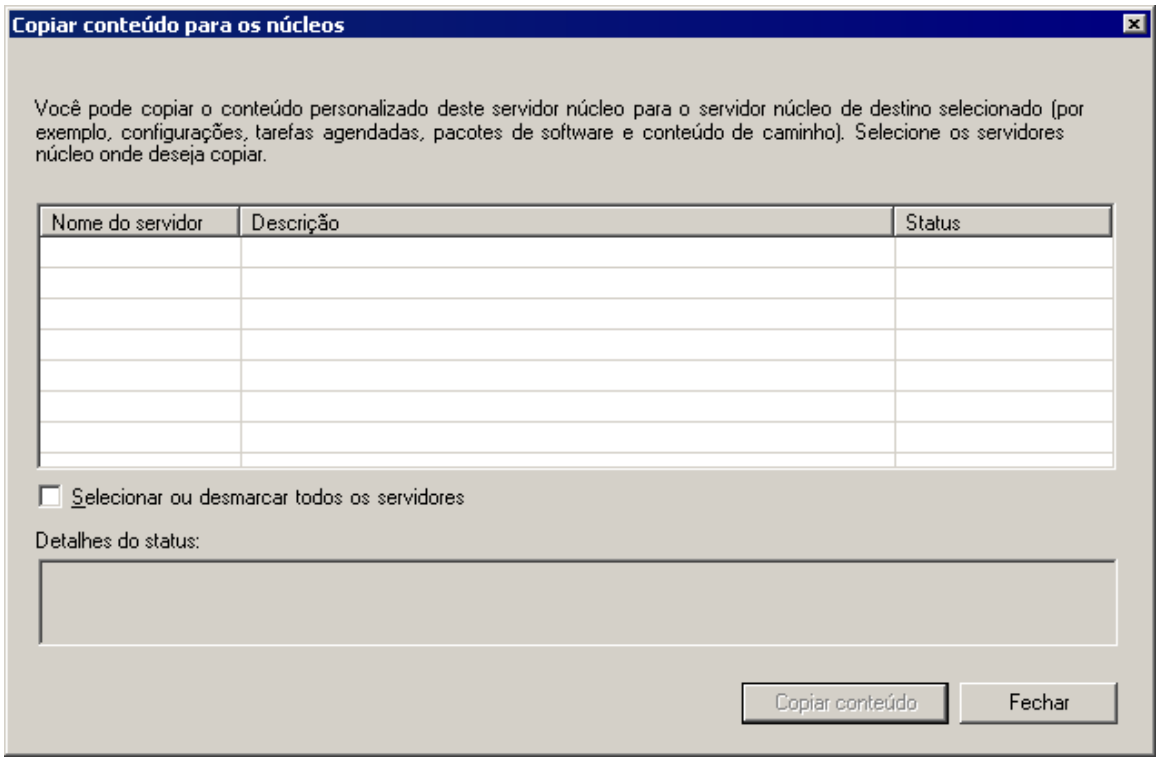
1. Clique em **Ferramentas > Administração > Sincronização de núcleo**.
2. Clique com o botão direito no item de árvore **Servidores núcleo** e clique em **Adicionar núcleo alvo**.
3. Insira o **Nome do núcleo**.
4. Selecione **Sincronizar a este núcleo** para habilitar a sincronização núcleo quando você sair do diálogo. É possível selecionar ou limpar esta opção mais tarde para habilitar ou desabilitar a sincronização seletivamente àquele núcleo.
5. Digite uma **Descrição**.
6. Digite um nome de domínio totalmente qualificado a ser usado pela conta do usuário durante a sincronização (domínio\nome do usuário). Esta conta deve ter privilégios de console e precisa ser membro de um dos grupos de usuários LANDesk locais no núcleo alvo.

7. Digite e confirme a **Senha** para a conta que você forneceu.
8. Clique em **Testar** para configur a a sua configuração.
9. Clique em **OK**.

IMPORTANTE: Os servidores de núcleo de rollup usam as credenciais de serviço do agendador para autenticar para fazer a sincronização. Nos núcleos de rollup essas credenciais de serviço do agendador precisam ser membros de um grupo com privilégios de administrador do console nos servidores núcleos de origem. Se as credenciais não tiverem esses privilégios, você verá erros no handler de tarefa no log de sincronização do núcleo de origem. Para ver informações sobre como mudar as credenciais do agendador, consulte "Sobre a caixa de diálogo Alterar login" na página 86.

Sincronizar itens por demanda

Use a sincronização de núcleo para sincronizar um item por demanda clicando nele com o botão direito e clicando em **Copiara para outro(s) núcleo(s)**. Ao fazer isso, você pode selecionar os servidores que deseja que recebam a cópia. Quando você clica em **Copiar conteúdo** isso inicia imediatamente a operação de cópia. A cópia só ocorre uma vez e o item que você copiou fica disponível imediatamente nos núcleos remotos. Você pode ter que atualizar manualmente o modo de exibição do núcleo do console pressionando F5 para o item aparecer. As cópias remotas têm o mesmo nome e local da cópia de origem e são editáveis. Os grupos ou subgrupos que contêm o item serão criados automaticamente.


Copiar conteúdo para os núcleos
Você pode copiar o conteúdo personalizado deste servidor núcleo para o servidor núcleo de destino selecionado (por exemplo, configurações, tarefas agendadas, pacotes de software e conteúdo de caminho). Selecione os servidores núcleo onde deseja copiar.
Nome do servidor
Descrição
Status
Selecionar ou desmarcar todos os servidores
Detalhes do status:
Copiar conteúdo
Fechar

Sincronizar itens automaticamente

Antes de usar a sincronização automática, configure os componentes Management Suite que você quer sincronizar.

Configurar a sincronização automática

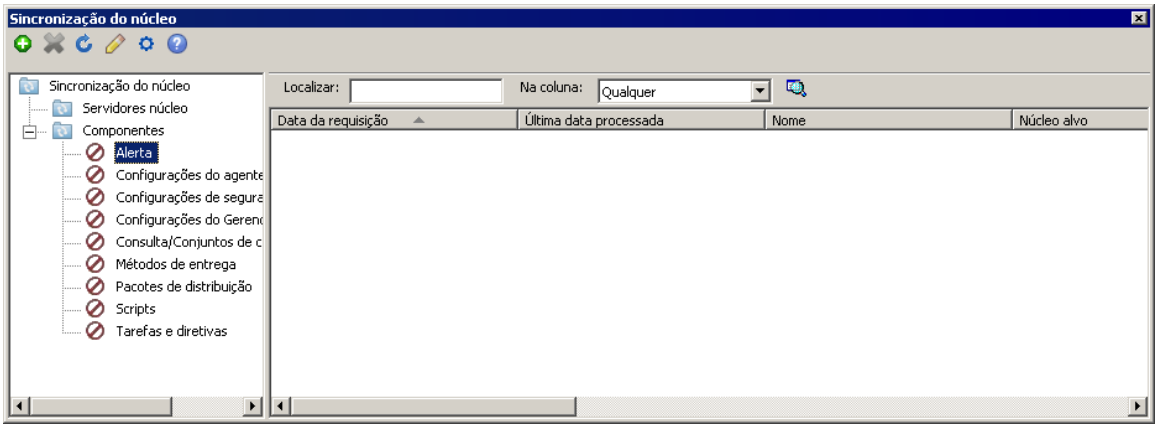
Você pode habilitar a sincronização automática em itens individuais, mas se um componente do item tiver a sincronização habilitada, esse item não será sincronizado. A desativação da sincronização em um componente não muda o sinalizador de sincronização automática nos itens sinalizados, por isso, se você desativar e posteriormente ativar a sincronização, os itens para os quais você habilitou a sincronização automática continuarão a sincronização.

Para selecionar os componentes com sincronização automáticoa que você habilitou

1. Clique em **Ferramentas > Administração > Sincronização de núcleo**.
2. Clique com o botão direito no item da árvore de **Componentes** e clique em **Editar componentes de sincronização automática**.
3. Mude os componentes que deseja sincronizar para a lista **Componentes de sincronização automática**.
4. Clique em **OK**.

Você pode também habilitar ou desabilitar a sincronização automática clicando com o botão direito em um componente e clicando em **Sincronização automática**.

Quando você seleciona um componente na árvore de **Componentes**, você vê a atividade de sincronização daquele componente.



Habilitação da sincronização automática para um item

Sincronize um item automaticamente clicando com o botão direito nele em uma tela de árvore de componente e clicando em **Sincronização automática**. Se o componente de sincronização do item não estiver habilitado você será avisado a habilitar aquele componente. A sincronização para esse item ocorrerá na próxima sincronização. Se você clicar com o botão direito outra vez nesse item, você verá uma marca próxima a **Sincronização automática** no menu.

Como no caso da sincronização por demanda, a sincronização automática de itens aparece no mesmo local no console. Entretanto, os itens automaticamente sincronizados nos núcleos alvo são apenas para leitura e não podem ser editados ou apagados. Toda vez que você muda um item de sincronização automática no núcleo de origem, o item é sincronizado com os núcleos alvo. Se você quiser que os usuários do console possam apagar um item sincronizado automaticamente, desative a sincronização automática. Isso não remove o item dos núcleos alvo, mas esses itens alvo tornar-se-ão editáveis.

Tarefas de sincronização agendadas

Os dados da tarefa de sincronização agendada não incluem a hora de início da tarefa. Se você sincronizar uma tarefa agendada, o único jeito de executá-la no servidor alvo é clicar nela com o botão direito e clicar em **Iniciar agora**. Como os itens sincronizados são do tipo somente-leitura, você não pode editá-los no núcleo alvo, nem adicionar uma nova hora de início. Como solução temporária você pode usar o recurso de cópia no núcleo. A tarefa ainda não incluirá a hora de início no núcleo alvo, mas dessa forma a tarefa será ali editável.

Exportar e importar itens de sincronização de núcleo

Os itens que você pode sincronizar pode também ser exportados e importados. A exportação de um item criar um arquivo .ldms no formato XML que contém os dados necessários para recriar esse item e qualquer item por ele referenciado. Você pode, então, mudar esse arquivo para outro núcleo, por exemplo, reimportá-lo.

Ao importar, você será avisado a fazer uma de três coisas:

- **Atualizar:** Inserir ou atualizar itens correspondentes, manter a hierarquia do grupo especificado no arquivo .ldms. Preserva as IDs do arquivo. Isso substitui as mudanças no item existente.
- **Inserir itens nos grupo ou proprietário selecionado:** Insira todos os itens e atribua novos IDs a cada um. Só adicione ao grupo se o tipo corresponder. Atualize o proprietário de cada item importado.
- **Inserir itens em grupos especificados no arquivo .ldms:** Insira os novos itens e mantenha a hierarquia do grupo especificado no arquivo .ldms. Novos IDs são atribuídos a cada item.

Para obter mais informações sobre como o gerenciamento de conflito funciona, consulte "Gerenciamento de conflito de sincronização de núcleo" na página 97.

Para exportar um item

1. Na **Tela de rede** ou na tela da árvore de ferramenta, clique com o botão direito no item que deseja exportar e clique em **Exportar**. Se um item for exportável ele terá um comando **Exportar**.
2. Digite um nome de arquivo e navegue para o caminho que desejar.
3. Clique em **Salvar**.

Para importar um item

1. Na **Tela da rede** ou na tela da árvore de ferramenta, navegue para o local onde deseja que o item importado apareça.
2. Clique com o botão direito e clique em **Importar**.
3. Clique na opção importar que deseja.
4. Clique em **Importar**.

Monitoração de status de sincronização de núcleo

Quando você seleciona um **Servidor núcleo** ou **Componente** na tela da árvore da ferramenta de Sincronização de núcleo, você pode ver um log de sincronizações e status de sincronização em tempo real. Role para a direita para ver as colunas de status disponíveis. Quando você seleciona o nó raiz dos **Servidores núcleo**, você pode ver um status de alto nível de sincronização para os núcleos alvo. Estes dados incluem a contagem pendente, que se for alta ou parada pode indicar que há um problema ao sincronizar esse núcleo.

Sincronize itens que têm um ou dos seguintes estados:

- **Pendente:** O item está esperando para ser enviado.
- **Enviar:** O item foi enviado.
- **Funcionando:** O núcleo de origem está processando o item.
- **Bem sucedido:** O item foi sincronizado com êxito.
- **Com falha:** O item não foi sincronizado.

Gerenciamento de conflito de sincronização de núcleo

Itens exportáveis de núcleo têm um ID exclusivo que ajuda o Management Suite a saber se os itens são os mesmos ou não. Isso ajuda a sincronizar conflitos de itens sincronizados. Se você copia ou sincroniza um item em um servidor e este mesmo item existe no servidor algo, aquele item será substituído somente se os itens compartilharem a mesma ID única. A ID única consiste do nome do servidor núcleo e do número da linha do banco de dados contendo o item. Você pode ver um ID exclusivo de item e o número de revisão em um diálogo de informações (clique com o botão direito no item e clique em **Info**).

Se dois itens com o mesmo nome tiverem IDs diferentes, a sincronização deixará o original intacto no alvo e adiciona a %1 para sincronizar o nome do arquivo do item sincronizado. A sincronização continua criando novas entradas em subsequentes conflitos de sincronização e incrementa esse número para cada um até o limite de 99 ser atingido.

Mudar as configurações de sincronização automática

Você pode configurar o intervalo de sincronização automático do servidor núcleo. O intervalo padrão é de dois minutos. Quando o seu intervalo selecionado tiver passado, o servidor núcleo marca os itens sincronizados automaticamente para mudanças. Se algum deles tiver mudado, o núcleo envia essas mudanças para os núcleos alvo que você especificou. Dependendo da quantidade de dados sendo sincronizados, diminuir esse intervalo ligeiramente aumenta a carga do processador do núcleo de origem.

A caixa de diálogo Configurações de Sincronização automática contém estas duas opções:

- **Sincronizar a cada:** O intervalo de sincronização que você deseja. O intervalo padrão é de dois minutos.
- **Número máximo de tentativas:** O número de vezes que este núcleo tentará conectar-se aos núcleos alvo. O padrão é cinco. Quando esse limite é alcançado, o núcleo de origem não tentará mais sincronizar aquele item.
- **Compacte os dados ao enviar:** O núcleos sincronizam via HTTPS. Quando marcada, esta opção também compacta o fluxo de dados. O padrão é selecionado.
- **Mostrar avisos de apenas leitura quando o usuário tentar editar itens sincronizados automaticamente:** Esta opção se aplica apenas ao servidor onde você fez essa mudança e ela se refere a itens sincronizados automaticamente que este servidor recebe e não origina. Você pode desativar esta opção se não quiser que os usuários do console vejam um aviso a mais se tentarem fazer uma mudanças em um item sincronizado automaticamente neste servidor. Desmarcar esta opção só desativa o aviso extra. Os usuários do console não poderão mudar os itens sincronizados automaticamente que o servidor recebe.

Para mudar as configurações de sincronização automática

1. Clique em **Ferramentas > Administração > Sincronização de núcleo**.
2. Na barra de ferramentas da ferramenta **Sincronização de núcleo**, clique no botão **Editar configurações de serviço de sincronização**.
3. Digite o intervalo de sincronização que você deseja.
4. Mude as outras opções se necessário.
5. Clique em **OK**.

Para reinicar a sincronização em um item que excedeu o limite de tentativas

1. Clique em **Ferramentas > Administração > Sincronização de núcleo**.
2. Em **Servers núcleo**, clique servidor em que você deseja reiniciar a sincronização.
3. No log, clique com o botão direito no item que falhou e clique em **Sincronizar novamente**.

Configuração de agentes

Configuração de agentes de dispositivo

Os dispositivos precisam que Management Suite os agentes sejam completamente gerenciáveis. Este capítulo contém informações sobre:

- "Usar configurações de agente" na página 101
- "Crie uma configuração de agente" na página 102
- "Uso do agente avançado" na página 104
- "Atualizar as preferências de agentes em dispositivos" na página 107
- "Criar pacotes independentes de configuração de agentes" na página 107
- "Segurança de agente e certificados confiáveis" na página 108
- "Remoção de agentes de dispositivo" na página 112

A janela **Configuração do agente** permite criar novas configurações de agentes para dispositivos Windows, Linux e Macintosh. As configurações de agentes que você criar podem então ser enviadas a clientes com o uso da janela **Tarefas agendadas** do console.

NOTA: A distribuição de agentes para dispositivos do Windows 95/98/NT
Management Suite não disponibiliza mais agentes que suportam dispositivos do Windows 95, Windows 98 ou Windows NT. É possível entrar em contato LANDesk com o Atendimento ao Cliente caso haja necessidade de agentes antigos que funcionem com esses dispositivos.

NOTA: Criação de configurações de dispositivo para dispositivos Windows não habilitados para gerenciamento
Caso existam dispositivos do Windows que sejam parte de um domínio Windows, você pode instalar uma configuração nesses clientes por envio, mesmo se o agente padrão LANDesk e os agentes do Controle remoto não estiverem presentes. Mais informações estão disponíveis na documentação de distribuição na comunidade LANDesk http://community.landesk.com.

NOTA: Agente de configuração em ambientes de vários idiomas
Ao criar configurações de agente em ambientes de vários idiomas verifique se o nome da configuração de agente está em ASCII (código padrão americano para troca de informações). Um servidor núcleo em inglês é compatível com clientes em qualquer idioma com suporte. Entretanto, se o nome da configuração de agente usa caracteres não-ASCII, como japonês, chinês ou russo, a configuração de agente precisa ser criada em um núcleo/console com o mesmo idioma e só funcionará em dispositivos que usam o mesmo idioma. Por exemplo, uma configuração de agente que contém caracteres japoneses precisa ser criada em um núcleo japonês e precisa ser distribuído para um cliente japonês.

Configurar descoberta de agentes

A Descoberta de agente é o processo usado para localizar dispositivos gerenciados que tenham o agente padrão ou agente de controle remoto instalados. Esses dois agentes fornecem os seguintes recursos:

- **O agente LANDesk padrão:** Habilita o PDS (serviço de descoberta de ping). Se o agente padrão estiver instalado em um dispositivo, será possível agendar as distribuições de software e as

configurações de instalação de dispositivos.

- **Controle remoto:** permite acessar e controlar remotamente um dispositivo.

A descoberta de agentes usa TCP/IP para verificar os agentes em execução nos dispositivos.

Os endereços IP são usados como critérios de pesquisa para realizar a descoberta do agente padrão do LANDesk com TCP/IP. A Management Suite procura o agente LANDesk padrão e o agente de controle remoto em dispositivos dentro de um intervalo específico de endereços IP. Esse intervalo de endereços é implícito pelo endereço de rede IP fornecido.

Se você não designar endereços de rede para sub-redes quando pesquisar por TCP/IP, a descoberta é realizada somente no segmento da rede onde reside o console que inicia a descoberta. Por exemplo, se você instalou quatro consoles de gerenciamento, cada um residindo em segmentos diferentes da rede, deverão ser feitas quatro análises, uma para cada console.

Nos segmentos da rede em que não existem consoles de gerenciamento, você deve usar endereços de sub-redes para acessar as informações sobre esses segmentos de rede.

NOTA: Se você tiver uma ou mais firewalls em sua rede, a descoberta de agente não pode ser usada para pesquisar fora das firewalls, pois elas geralmente limitam o fluxo do tráfego de pacotes às portas designadas.

O padrão de descoberta de agente é fazer a descoberta somente do dispositivo selecionado. Você pode ajustar as opções de descoberta seguindo os passos abaixo.

Para configurar as opções de descoberta de agentes:

1. Clique em **Configurar** > **Opções de status do agente**.
2. Selecione as opções de descoberta e de atualização desejadas. Para mais informações, consulte a próxima seção.
3. Clique em **OK**.

Sobre o diálogo Opções de status de agente

Use essa caixa de diálogo para configurar as seguintes opções de descoberta de agentes.

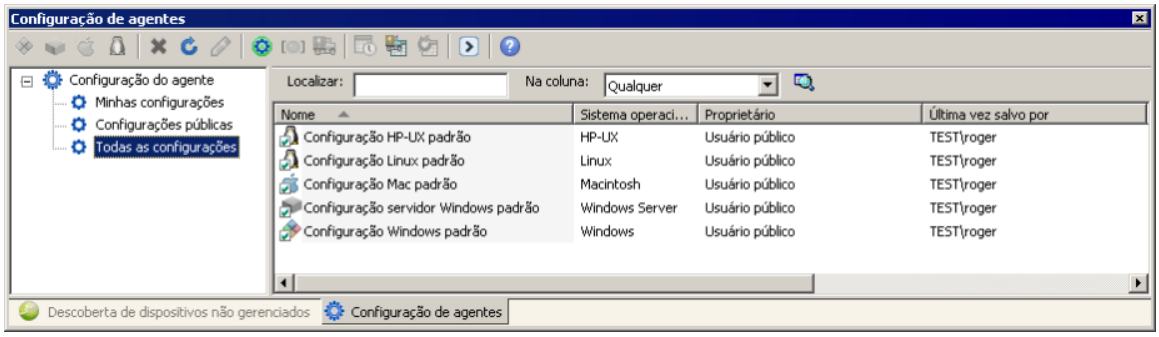
- **Coletar status de agente:**
  - **Nunca:** Nunca reúna o status do agente. Use esta opção se você tiver muitos dispositivos não confiáveis ou um link de rede fraco.
  - **Somente para os itens selecionados visíveis:** Especifica que o status do agente de um dispositivo será atualizado quando o dispositivo for selecionado na tela de rede. Considere usar esta opção e desativar a atualização automática se a relação entre os dispositivos disponíveis e indisponíveis for aproximadamente meio-a-meio. Usar esta opção e desativar a atualização automática também é bom quando você quer reduzir a quantidade de tráfego de rede gerado pelo console.
  - **Para todos itens visíveis:** Especifica que todos os dispositivos visíveis na Tela de rede terão o status do agente atualizado de acordo com a taxa de atualização. À medida que novos dispositivos se tornam visíveis, seu status de agente (e condição) é atualizado. Esta opção gera a maior parte do tráfego de rede.

- **Atualizar a cada < > minutos:** Indica se o status do agente é atualizado automaticamente no intervalo selecionado. Para ativar essa opção, selecione a caixa de seleção ao lado de **Atualizar**. Por padrão, essa opção está desabilitada e o intervalo de atualização só é aplicável se a caixa de seleção estiver selecionada. Se você ativar isto, considere usar o intervalo padrão de 5 minutos, ou mais, para reduzir a quantidade de tráfego de rede.

Usar configurações de agente

Management Suite utiliza as configurações de agentes que você criou para distribuir agentes e preferências de agentes para dispositivos gerenciados. Assim que os dispositivos tiverem os agentes do Management Suite neles, é fácil atualizar as configurações de agentes.

A ferramenta Configuração do agente é usada para criar e atualizar as configurações de agente de dispositivo e de servidor (por exemplo, o agentes que são instalados nos dispositivos e os protocolos de rede que os agentes utilizam). Diferentes configurações podem ser criadas para necessidades específicas de departamentos ou grupos. Por exemplo, podem ser criadas configurações para os dispositivos no departamento de contabilidade ou para dispositivos usando um determinado sistema operacional. Só pode haver uma configuração padrão para cada tipo de configuração. A configuração padrão não pode ser excluída, mas pode ser editada. É uma boa idéia não ter muitas configurações diferentes, pois isso torna o suporte e a resolução de problemas mais complexos e demorados.



Antes de instalar qualquer software agente é necessário criar uma configuração de agente (ou usar a padrão). Isso requer considerável planejamento e teste. É melhor distribuir a configuração correta na primeira vez - embora o agente possa também ser reconfigurado e redistribuído novamente se necessário.

Uma empresa pode precisar de múltiplas configurações de agente. Por exemplo, um sistema de laptops pode precisar de uma configuração diferente da configuração de um sistema de desktops. Para evitar distribuir o agente errado para o sistema errado é importante adotar uma convenção de nomenclatura adequada para cada configuração de agente.

O agente de análise de segurança e correção é instalado como padrão com o agente LANDesk padrão. Você pode configurar as análises de segurança para determinar como e quando são executadas nos dispositivos gerenciados e se devem ou não mostrar as opções interativas e de progresso ao usuário final. (O analisador de segurança permite a verificação de atualizações de software do LANDesk nos dispositivos e servidores núcleo mesmo se você não tiver uma LANDesk Security Suite assinatura de conteúdo. Com a assinatura do Security Suite, você pode aproveitar as vantagens plenas da capacidade da análise de segurança para analisar e corrigir vulnerabilidades conhecidas, spyware, aplicativos não autorizados e outros riscos potenciais de segurança.)

Antes de distribuir o agente, consulte as melhoras práticas de distribuição no site da Comunidade de usuários da LANDesk em http://community.landesk.com/support/docs/DOC-23482.

IMPORTANTE: Ao criar configurações de agente em ambientes de vários idiomas verifique se o nome da configuração de agente está em ASCII (código padrão americano para troca de informações). Um servidor núcleo em inglês é compatível com clientes em qualquer idioma com suporte.

Entretanto, se o nome da configuração de agente usa caracteres não-ASCII, como japonês, chinês ou russo, a configuração de agente precisa ser criada em um núcleo/console com o mesmo idioma e só funcionará em dispositivos que usam o mesmo idioma. Por exemplo, uma configuração de agente que contém caracteres japoneses precisa ser criada em um núcleo japonês e precisa ser distribuído para um cliente japonês.

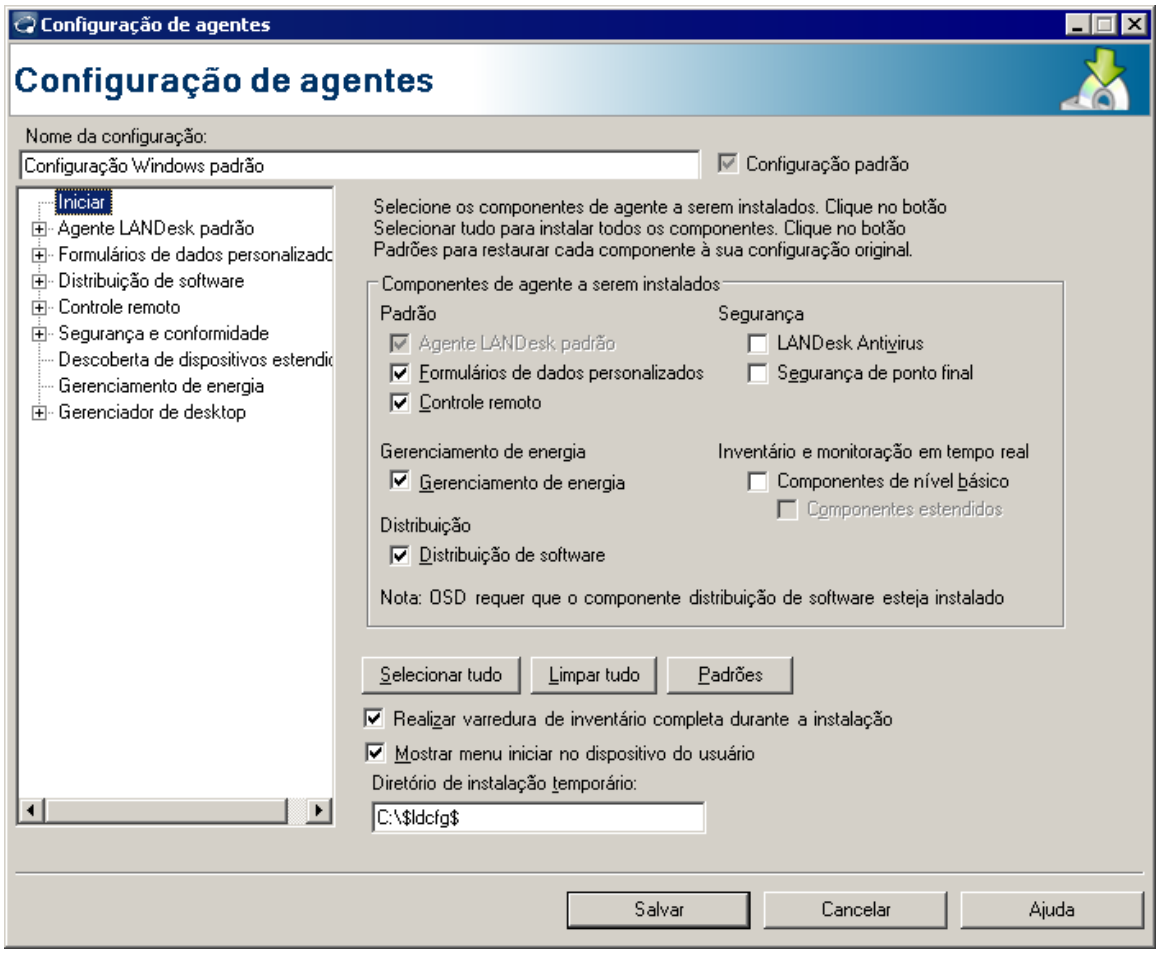
Para obter mais informações, leia as seguintes seções:

- "Crie uma configuração de agente" na página 102
- "Uso do agente avançado" na página 104
- "Atualizar as preferências de agentes em dispositivos" na página 107

Crie uma configuração de agente

Use a janela **Configuração do agente** para criar e atualizar as configurações de agente de dispositivo e de servidor (por exemplo, o agentes que são instalados nos dispositivos e os protocolos de rede que os agentes utilizam).

Você pode criar diferentes configurações para necessidades específicas do grupo. Por exemplo, você pode criar configurações para os dispositivos no departamento de contabilidade ou para clientes usando um determinado sistema operacional.



Para instalar por envio uma configuração nos dispositivos, é necessário:

- **Criar a configuração de agentes:** Definir configurações específicas para seus dispositivos. Em geral uma "configuração de agente avançada" é a melhor escolha. Para obter mais informações, consulte a próxima seção, "Uso do agente avançado" na página 104.
- **Agendar a configuração do agente:** Instalar por envio a configuração nos dispositivos com o agente LANDesk padrão instalado. Usuários com direitos administrativos também podem instalar a configuração do agente padrão executando o arquivo wscfg32.exe ou IPSETUP.BAT no compartilhamento LDLogon do servidor núcleo.

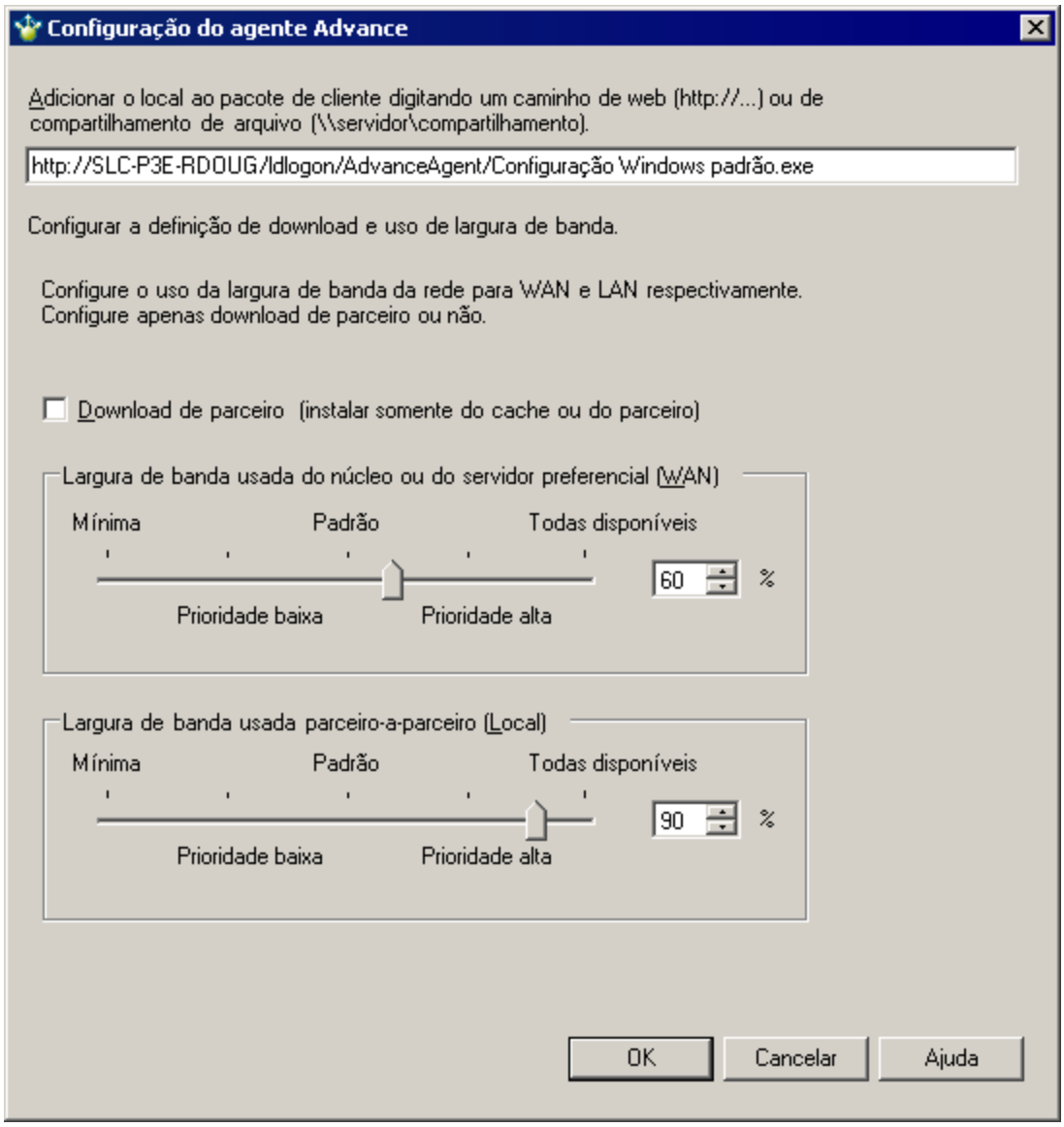
Para criar uma configuração de agentes

1. No console, clique em **Ferramentas > Configuração > Configuração de agentes**.
2. Na árvore **Configuração de agentes**, clique na categoria de configurações que desejar.
3. Clique no botão da barra de ferramentas **Novo Windows, Novo servidor Windows, Novo Macintosh** ou **Novo Linux**.
4. Digite um **Nome de configuração**.
5. Na página **Iniciar** da janela **Configuração de agentes**, selecione os agentes que desejar distribuir.

6. Use a árvore para navegar para as caixas de diálogo relacionadas às opções que selecionar. Personalize as opções que selecionou conforme necessário. Clique em **Ajuda** para obter mais informações caso haja dúvidas sobre uma página.
7. Clique em **Salvar**.
8. Se desejar que a configuração seja a configuração padrão (as configurações ldlogon\wscfg32.exe ou ldlogon\IPSETUP.BAT serão instaladas), clique em **Configuração padrão** no menu de atalho da configuração.

Uso do agente avançado

O agente avançado é o método preferencial para distribuição do agente na maioria dos ambientes. O Agente avançado foi criado para aproveitar as vantagens da tecnologia compatível com largura de banda da LANDesk durante a distribuição do agente. Ele pode reduzir a quantidade de largura de banda utilizada para a configuração do agente baseado em Windows. O Agente avançado usa um método de distribuição de dois estágios. O Agente avançado é um arquivo MSI que é distribuído antes do agente inteiro. O MSI é instalado e, então, dá início ao download e instalação do pacote completo do agente.


Configuração do agente Advance
Adicionar o local ao pacote de cliente digitando um caminho de web (http://...) ou de compartilhamento de arquivo (\\servidor\compartilhamento).
http://SLC-P3E-RDOUG/ldlogon/AdvanceAgent/Configuração Windows padrão.exe
Configurar a definição de download e uso de largura de banda.
Configure o uso da largura de banda da rede para WAN e LAN respectivamente.
Configure apenas download de parceiro ou não.
Download de parceiro (instalar somente do cache ou do parceiro)
Largura de banda usada do núcleo ou do servidor preferencial (WAN)
Mínima
Padrão
Todas disponíveis
60
%
Prioridade baixa
Prioridade alta
Largura de banda usada parceiro-a-parceiro (Local)
Mínima
Padrão
Todas disponíveis
90
%
Prioridade baixa
Prioridade alta
OK
Cancelar
Ajuda

O agente avançado funciona bem com a maioria dos dispositivos, inclusive laptops com conexões de rede intermitentes ou lentas. O agente avançado não é compatível com PDAs e outros dispositivos de mão.

O agente avançado é um pacote .MSI pequeno de 500 KB. Quando este pacote é executado em um dispositivo gerenciado, ele descarrega um pacote de configuração de agente completo, o qual pode ter até 15 MB, dependendo dos agentes selecionados. Na caixa de diálogo **Configuração de agente avançado** você pode configurar as opções de distribuição compatíveis com largura de banda que o .MSI utilizará para o download da configuração completa de agente.

O agente avançado funciona independente do servidor núcleo quando começa a descarregar a configuração completa de agente. Se um dispositivo desconecta da rede antes do download da configuração do agente terminar, o agente avançado continua o download automaticamente assim que o dispositivo estiver novamente conectado à rede.

Quando você cria uma configuração de agente avançado, demora alguns segundos para o console criar o pacote de configuração completa de agente. O console coloca o pacote do agente avançado (<nome da configuração>.msi) e o pacote de configuração completa de agente recém-criado (<nome da configuração>.exe) na pasta LDLogon\AdvanceAgent do servidor núcleo. Os nomes de arquivo são baseados no nome de configuração do agente.

Após criar um pacote de configuração de agente, é necessário executar a parte .MSI nos dispositivos através de um dos seguintes métodos:

- Agende a parte pequena do .MSI para uma distribuição forçada.
- Execute o .MSI manualmente em cada dispositivo.
- Configure manualmente o .MSI para ser executado via script de login.

Ao distribuir o agente avançado para os dispositivos, ele inicia o download da configuração associada do agente. O agente é executado silenciosamente no dispositivo gerenciado, sem mostrar nenhuma caixa de diálogo ou atualização de status. O agente avançado utiliza as preferências de largura de banda especificadas na caixa de diálogo **Configuração do agente avançado**, por exemplo, Download de parceiro e aceleração de largura de banda dinâmica.

Após instalar e configurar os agentes corretamente no dispositivo, o .MSI remove o pacote de configuração completa de agente. A parte do .MSI fica no dispositivo e, caso seja executado novamente, ele não reinstala os agentes.

Criar uma configuração de agente avançada

Para criar uma configuração de agente avançado

1. Crie uma configuração de agente baseado em Windows (**Ferramentas | Configuração | Configuração do agente**).
2. No menu de atalho dessa configuração, clique em **Agente avaçado**.
3. Selecione as opções desejadas.
4. Se você selecionar **Download de parceiro**, deve confirmar que o arquivo .msi do agente avançado e o pacote completo de configuração de agente .exe estão no cache de distribuição do software de um dispositivo no domínio de transmissão. Se você selecionar **Download de parceiro** e não fizer isso antes de distribuir a configuração do agente avançado, a distribuição falhará porque está sem cache ou o parceiro não possui os arquivos necessários no domínio de transmissão.
5. Se estiver transferindo o pacote associado de configuração de agente (o arquivo .exe) para outro lugar, mude o caminho para o pacote de configuração do agente, de forma a corresponder ao novo local.
6. Clique em **OK**.
7. Se necessário, copie o arquivo .exe associado da pasta LDLogon\AdvanceAgent para o servidor de distribuição. Assegure-se de que o caminho ao executável da configuração do agente corresponde ao caminho especificado na caixa de diálogo **Configuração de agente avançado**. O pacote MSI deve ser deixado no servidor núcleo no local padrão. Caso contrário, o pacote não será visível à tarefa de distribuição forçada do agente avançado abaixo.

Para configurar uma distribuição forçada de agente avançado

1. Na janela Configuração do agente (**Ferramentas > Configuração > Configuração de agente**), clique no botão**Agendar uma instalação forçada de configuração de agente avançado.**.

2. A caixa de diálogo **Configurações do agente avançado** mostra as configurações de agente existentes na pasta LDLogon\AdvanceAgent. Clique na configuração que deseja distribuir e clique em **OK**.
3. A janela **Tarefas agendadas** abre-se com a tarefa de agente avançado que você criou, selecionada. O nome da tarefa é o "Agente avançado da <nome da sua configuração>".
4. Adicione dispositivos alvo à tarefa arrastando-os da tela de rede e soltando-os na tarefa que quiser na janela **Tarefas agendadas**.
5. No menu de atalho da tarefa, clique em **Propriedades** e agende a tarefa. Veja o andamento da distribuição da parte MSI na janela **Tarefas agendadas**. Não há atualizações de status na configuração completa de agente quando a distribuição do MSI termina.

Atualizar as preferências de agentes em dispositivos

Se você desejar atualizar as preferências de agentes em dispositivos, por exemplo, exigir permissão para controle remoto, não é necessário redistribuir a configuração inteira dos agentes. Faça as mudanças que desejar na janela **Configuração do agente** e nesse menu de atalho da configuração clique em **Agendar atualização**. Essa ação abre a janela **Tarefas agendadas** e cria uma tarefa e um pacote de atualização para a configuração de onde a atualização foi agendada. Esse pacote tem apenas algumas centenas de quilobytes de tamanho.

A atualização de preferências não instala ou remove agentes no dispositivo. Se a atualização contiver preferências para agentes que não se encontram no dispositivo, as preferências que não se aplicarem serão ignoradas.

IMPORTANTE: O Agent Watcher não permite a alteração de preferências durante as atualizações programadas. Se você quiser alterar as preferências do Agent Watcher, clique com o botão direito no dispositivo desejado na Tela de rede e clique em **Atualizar as configurações do Agent Watcher**.

Para atualizar as preferências de agentes em dispositivos

1. Clique em **Ferramentas > Configuração > Configuração de agentes**.
2. Personalize a configuração que você desejar usar.
3. Ao terminar, clique em **Agendar atualização das configurações de agentes** no menu de atalho da configuração. Isto abre a janela **Tarefas agendadas**.
4. Selecione os dispositivos que desejar atualizar e agende a tarefa.

Criar pacotes independentes de configuração de agentes

Normalmente o utilitário de configuração do cliente, o wscfg32.exe, configura clientes. Se você desejar, é possível fazer a janela de **Configuração de agentes** criar um único arquivo executável de auto-extração que instala a configuração de agentes no dispositivo em que for executado. Isso é útil se você desejar instalar agentes de um CD ou de uma unidade USB portátil, ou se desejar fazer multidifusão de uma configuração de agentes.

Para criar um pacote independente de configuração de agentes

1. Clique em **Ferramentas > Configuração > Configuração de agentes**.
2. Personalize a configuração que você desejar usar.

3. Quando terminar, clique em **Criar pacote de instalação de cliente** no menu de atalho da configuração.
4. Selecione o caminho do local onde deseja que o pacote seja armazenado. Certifique-se que o nome do arquivo contenha apenas caracteres ASCII (a-z, A-Z, 0-9).
5. Aguarde o Management Suite criar um pacote. Isto leva alguns minutos.

Segurança de agente e certificados confiáveis

Management Suite 8 usa um sistema de autenticação baseado em certificados. Os agentes do dispositivo se autenticam em servidores núcleo autorizados, evitando o acesso de núcleos não autorizados aos clientes. Cada um dos servidores núcleo possui um certificado e uma chave privada exclusivos que a Instalação do Management Suite cria na primeira instalação do núcleo ou do servidor núcleo de rollup.

Estes são os arquivos de chave privada e de certificados:

- **<nome_da_chave>.key:** O arquivo .key é a chave privada do servidor núcleo e reside apenas no servidor núcleo. Se a privacidade desta chave for comprometida, o servidor núcleo e as comunicações com o dispositivo não estarão protegidas. Mantenha essa chave protegida. Por exemplo, não a envie por-email para mover.
- **<nome_da_chave>.crt:** O arquivo .crt contém a chave pública do servidor núcleo. O arquivo .crt é uma versão da chave pública que pode ser visualizada para se obter mais informações.
- **<hash>.0:** O arquivo .0 é um arquivo de certificado confiável cujo conteúdo é idêntico ao do arquivo .crt. Entretanto, seu nome é atribuído de forma a permitir que o computador localize rapidamente o arquivo de certificado em uma pasta com muitos certificados diferentes. O nome é um hash (checksum) das informações do certificado. Para determinar o nome de arquivo hash de um certificado específico, veja o arquivo <nome_da_chave>.crt. Existe uma seção [LDMS] do arquivo .ini no arquivo O par hash=value indica o valor de <hash>.

Um outro método de obter o hash é usar o aplicativo openssl, que está armazenado na pasta \Arquivos de programas\LANDesk\Shared Files\Keys. Ele mostrará o hash associado a um certificado, usando a seguinte linha de comando:

```
openssl.exe x509 -in <nome_da_chave>.crt -hash -noout
```

Todas as chaves são armazenadas no servidor núcleo em \Arquivos de programas\LANDesk\Shared Files\Keys. A chave pública <hash>.0 está também na pasta ldlogon e, como padrão, deve estar ali. <nome_da_chave> é um nome do certificado que você forneceu durante a instalação do Management Suite. É útil fornecer um nome descritivo durante a instalação, por exemplo, você pode utilizar o nome do servidor núcleo (ou mesmo o nome completo dele) para a chave (exemplo: ldcore ou ldcore.org.com). Isso facilitará a identificação dos arquivos de certificado/chave privada em um ambiente com vários núcleos.

Você deve fazer backup do conteúdo da pasta Keys (Chaves) do seu servidor núcleo em lugar seguro e protegido. Se, por alguma razão, for necessário reinstalar ou substituir o servidor núcleo, você não poderá gerenciar os dispositivos desse servidor núcleo até adicionar os certificados do núcleo original ao novo núcleo.

Compartilhamento de chaves entre servidores núcleo

Os dispositivos se comunicarão apenas com os servidores núcleo e servidores núcleo de rollup para os quais tiverem um arquivo de certificado confiável correspondente. Por exemplo, digamos que você tenha três servidores núcleo que gerenciem 5.000 dispositivos cada um. Você também tem um núcleo de rollup que gerencie todos os 15.000 dispositivos. Cada servidor núcleo terá seu próprio certificado e suas próprias chaves privadas e, por padrão, os agentes de dispositivos que você distribuir de cada servidor núcleo se comunicarão apenas com o servidor núcleo do qual o software do dispositivo é distribuído.

Existem duas formas principais de compartilhar chaves entre os servidores núcleo e núcleo de rollup:

1. Distribuição de cada certificado confiável de servidor núcleo (o arquivo <hash>.0) para dispositivos e seus respectivos servidores núcleo. Esta é a forma mais segura.
2. Cópia da chave privada e dos certificados para cada servidor núcleo. Isso não exige que você faça nada com os dispositivos mas, como é necessário copiar a chave privada, a exposição ao risco é maior.

No nosso exemplo, se você quiser que o núcleo de rollup e o console de Web sejam capazes de gerenciar dispositivos de todos os três núcleos, é necessário distribuir o certificado confiável do núcleo de rollup (o arquivo <hash>.0) para todos os dispositivos, além de copiar o mesmo arquivo para a pasta ldlogon de cada servidor núcleo. Para mais informações, consulte a próxima seção. Outra opção é copiar os arquivos de certificado/chave privada de cada um dos três servidores núcleo para o núcleo de rollup. Assim, cada dispositivo pode encontrar a chave privada correspondente ao seu servidor núcleo no servidor núcleo de rollup. Para obter mais informações, consulte "Copiar arquivos de certificados/chaves públicas entre servidores núcleo" na página 110.

Se você quiser que um servidor núcleo possa gerenciar dispositivos de outro servidor núcleo, siga o mesmo processo, distribuindo o certificado confiável a dispositivos ou copiando os arquivos de certificados/chaves públicas entre os núcleos.

Se estiver copiando certificados entre núcleos independentes (não um núcleo de rollup), há uma questão adicional. Um núcleo não consegue gerenciar dispositivos de outro núcleo a menos que haja antes uma varredura do inventário desses dispositivos. Uma maneira de passar varreduras de inventário para outro núcleo é agendar uma tarefa de varredura de inventário com uma linha de comando personalizada que encaminhe a análise para o novo núcleo. Em situações com vários núcleos, o uso de um núcleo de rollup e do Web console é a forma mais simples de gerenciar dispositivos entre núcleos. O núcleos de rollup obtêm automaticamente dados de varredura de inventário de todos os dispositivos dos núcleos que fazem rollup para eles.

Distribuição de certificados confiáveis para dispositivos

Existem duas formas de distribuir certificados confiáveis para dispositivos:

1. Distribuir uma configuração de dispositivo que tenha os certificados confiáveis do servidor núcleo que você quer.
2. Usar um trabalho de distribuição de software para copiar diretamente os arquivos de certificados confiáveis que você quiser para cada dispositivo.

Cada certificado confiável de servidor núcleo adicional (<hash>.0) que você quiser que os dispositivos usem deve ser copiado para o pasta ldlogon do servidor núcleo. Quando o certificado confiável estiver nesta pasta, você pode selecioná-lo a partir da página **Agente básico comum** do diálogo de configuração do dispositivo. A instalação do dispositivo copia as chaves para esta pasta nos seguintes dispositivos:

- Dispositivos Windows: \Arquivos de programas\LANDesk\Shared Files\cbaroot\certs
- Dispositivos Mac OS X: /usr/LANDesk/common/cbaroot/certs

Se você quiser incluir o certificado de um servidor núcleo em um dispositivo e não quiser redistribuir os agentes de dispositivo por meio da instalação do dispositivo, crie um trabalho de distribuição de software que copie o <hash>.0 para as duas pastas especificadas acima no dispositivo. Dessa forma, você pode usar a janela **Tarefas agendadas** para distribuir o script de distribuição de certificados que criou.

Veja a seguir um exemplo de um script personalizado que pode ser usado para copiar um certificado confiável da pasta ldlogon do servidor núcleo para um dispositivo. Para usá-lo, substitua "d960e680" pelo valor de hash do certificado confiável que você quer distribuir.

```
; Copie um certificado confiável do diretório ldlogon no servidor núcleo
; para o diretório de certificados confiáveis do cliente
[COMPUTADORES]
REMCOPY0=%DTMDIR%\ldlogon\d960e680.0, %TRUSTED_CERT_PATH%\d960e680.0
```

Copiar arquivos de certificados/chaves públicas entre servidores núcleo

Uma alternativa à distribuição de certificados (<hash>.0) para os dispositivos é copiar conjuntos de certificados/chaves privadas entre os núcleos. Os núcleos podem conter vários arquivos de certificado/chave pública. Desde que um dispositivo consiga autenticar-se com uma das chaves em um núcleo, ele pode comunicar-se com esse núcleo.

NOTA: Ao usar o controle remoto baseado em certificado, os dispositivos de destino devem estar no banco de dados núcleo
Se estiver usando segurança de controle remoto baseada em certificado com dispositivos, você só pode controlar remotamente os dispositivos que têm um registro do inventário no banco de dados ao qual está conectado. Antes de contactar um nó para disparar o controle remoto, o núcleo pesquisa o banco de dados para verificar se o solicitante tem direitos de ver o dispositivo. Se o dispositivo não estiver no banco de dados, o núcleo recusa a solicitação.

Para copiar um conjunto de certificados/chaves públicas de um servidor núcleo para outro

1. No servidor núcleo de origem, vá para a pasta \Arquivos de programa\LANDesk\Shared Files\Keys.
2. Copie os arquivos <nome_da_chave>.key, <nome_da_chave>.crt e <hash>.0 do servidor de origem para um disquete flexível ou outro local seguro.
3. No servidor núcleo de destino, copie os arquivos do servidor núcleo de origem para a mesma pasta (\Arquivos de programas\LANDesk\Shared Files\Keys). As chaves entram em vigor imediatamente.

Deve-se tomar cuidado para garantir que a chave privada <nome_da_chave>.key não seja comprometida. O servidor núcleo utiliza esse arquivo para autenticar os dispositivos e qualquer computador com o arquivo <nome_da_chave>.key pode realizar execuções remotas e transferência de arquivos para um dispositivo do Management Suite.

Distribuição de agentes para imagens não-persistentes de VDI

Ao distribuir agentes para imagens não-persistentes de VDI (Virtual Desktop Interface), existem alguns passos extras que você deve deve tomar.

O processo de configuração de agente adiciona entradas de registro do rastreamento do histórico de logon e de ID exclusivas para este dispositivo. Em um ambiente não-persistente, estes dados serão perdidos quando a imagem for redefinida.

Para garantir que o Management Suite rastreie cada máquina do pool de VDI individualmente, você deve excluir estas chaves de registro da imagem de base. Isto permite que as chaves de registro sejam recreadas quando cada máquina no pool de VDI inicia a primeira vez e os agentes carregam.

Essas são as chaves de registro de rastreamento de UniqueID e logon que você deve excluir da imagem de base de VDI.

Para imagens de VDI de 64 bits:

```
HKLM\SOFTWARE\Wow6432Node\Intel\LANDesk\CommonApi\UniqueID
HKLM\SOFTWARE\Wow6432Node\LANDesk\CommonApi\UniqueID
HKLM\SOFTWARE\Wow6432Node\LANDesk\Inventory\LogonHistory\Logons
```

Para imagens de VDI de 32 bits:

```
HKLM\SOFTWARE\Intel\LANDesk\CommonApi\UniqueID
HKLM\SOFTWARE\LANDesk\CommonApi\UniqueID
HKLM\SOFTWARE\LANDesk\Inventory\LogonHistory\Logons
```

Se estiver usando o monitoramento de uso do software, você também deve definir um caminho UNC onde os arquivos de dados de monitoramento serão armazenados. Se você não definir um caminho, o monitoramento de licença de software armazenará os dados de monitoramento no registro. Em um ambiente não-persistente, estes dados serão perdidos quando a imagem for redefinida.

Para gravar as estatísticas de uso do software em outro local na rede

1. Clique em **Ferramentas > Configuração de agente**.
2. Clique duas vezes na configuração de agente que você usará em sua imagem de VDI.
3. Clique em **Agente LANDesk padrão > Monitoramento de uso do software**.
4. Selecione **Usar monitoração de software**.
5. Selecione **Gravar as estatísticas de uso do software em outro local na rede**.
6. Insira as informações de caminho UNC e as credenciais que os agentes na imagem VDI devem usar para acessar o caminho UNC.
7. Salve as mudanças.
8. Distribua a configuração de agente para sua imagem de base de VDI.
9. Exclua as chaves de registro de rastreamento de UniqueID e logon mencionados anteriormente nesta seção.
10. Salve as mudanças na sua imagem de base de VDI.

Remoção de agentes de dispositivo

Antes do Management Suite 8.5, qualquer um podia desinstalar agentes do Management Suite executando o wscfg32 com o parâmetro /u. O wscfg32 estava no compartilhamento LDLogon, que podia ser acessado pelos dispositivos gerenciados, por isso era relativamente fácil para os usuários desinstalar os agentes Management Suite.

No Management Suite 8.5 e mais recente, o parâmetro /u foi removido do wscfg32. Há um novo utilitário denominado UninstallWinClient.exe no compartilhamento LDMain, que é a pasta principal de programa do ManagementSuite. Apenas os administradores têm acesso a esse compartilhamento. Esse programa desinstala os agentes do Management Suite ou do Server Manager em qualquer dispositivo em que é executado. Você pode mudá-lo para qualquer pasta que desejar ou adicioná-lo a um script de login. É um aplicativo Windows que é executado silenciosamente sem exibir nenhuma interface.

A execução desse programa não removerá um dispositivo do banco de dados. Se você redistribuir agentes para um dispositivo que executou esse programa, ele será armazenado no banco de dados como novo dispositivo.

Configuração de agentes de dispositivos Linux e UNIX

Você pode usar o LANDesk Management Suite para gerenciar distribuições suportadas para Linux/UNIX. Para obter mais informações sobre as versões Linux/UNIX suportadas e instruções de instalação, consulte a página de destino do LANDesk Linux\UNIX no site da Comunidade de usuários da LANDesk em http://community.landesk.com/support/docs/DOC-10608.

Ajuda dos dispositivos gerenciados

A janela da Configuração de agentes (**Ferramentas > Configuração > Configuração de agentes**) é onde você personaliza as configurações de agente do dispositivo. Use a caixa de diálogo Configuração de agentes para especificar os agentes que deseja instalar e as opção para esses agentes. Podem ser criadas quantas configurações de agente desejar. Entretanto, apenas uma pode ser a configuração padrão. Essa janela pode ser usada para criar as configurações de agente do Windows, Macintosh, Linux e de servidor.

Para criar uma configuração:

1. Clique em **Ferramentas > Configuração > Configuração de agentes**.
2. Clique no botão **Novo** para criar uma nova configuração de Windows. Clique no botão **Novo Mac** para criar uma nova configuração de Macintosh.
3. Preencha a caixa de diálogo **Configuração de agentes** conforme descrito nas seções a seguir. Clique em **Ajuda** em uma página para obter mais informações.

NOTA: Se você usar a caixa de diálogo **Configuração de agentes** para criar uma nova configuração de agente padrão, lembre-se de que todos os dispositivos configurados pelo WSCFG32 usando scripts de login serão reconfigurados automaticamente com os novos parâmetros padrão da configuração na próxima vez que se conectarem, mesmo se suas configurações atuais coincidirem com as novas configurações padrão.

As seções a seguir descrevem as páginas da caixa de diálogo Configuração de agentes.

Sobre a página Inicial

A página inicial da Caixa de diálogo configuração de agente contém as seguintes opções:

- **Nome de configuração:** Esta opção é exibida acima de todas as páginas da caixa de diálogo. Digite um nome que descreva a configuração em que você está trabalhando. O nome pode ser o nome de uma configuração existente ou um novo nome. Esse nome é exibido na janela **Configuração de agentes**.
- **Configuração padrão:** Quando selecionada, faz com que essa configuração seja a configuração instalada quando nenhuma outra for especificada.

Componentes de agente a instalar (Padrão):

- **Agente padrão do LANDesk:** Instala o agente LANDesk padrão que forma a base da comunicação entre os dispositivos e o servidor núcleo. Essa opção é obrigatória. Você não pode desativá-la, mas pode personalizar os componentes a ele associados. (Observe que o analisador de segurança é instalado automaticamente com o agente padrão do LANDesk, mas pode ser configurado com as opções de análise de segurança e patch abaixo.)
- **Formulários de dados personalizados:** Apresenta um formulário para os usuários preencherem. Você pode consultar o banco de dados núcleo para obter os dados inseridos pelos usuários. Use-o para recuperar informações personalizadas diretamente dos usuários.
- **Controle remoto:** Permite controlar um dispositivo ou servidor na rede. Minimiza o tempo utilizado para resolver questões dos clientes de um suporte técnico centralizado. Use-o para o gerenciamento remoto de dispositivos na LAN/WAN.

Gerenciamento de energia:

- **Gerenciamento de energia:** Permite controlar o consumo de energia nos seus computadores gerenciados de um local central. É possível criar e distribuir com facilidade diretivas de gerenciamento de energia e gerar relatórios para avaliar a economia financeira e de energia. Controle as condições de espera, hibernação ou desligamento de computadores e monitores. Entretanto, os usuários podem atrasar as ações específicas de gerenciamento de energia usando uma interface de usuário no cliente para assegurar que os dados não salvos sejam protegidos.

Distribuição:

- **Distribuição de software:** Automatiza o processo de instalação dos aplicativos de software ou de distribuição de arquivos para os dispositivos. Use-o para instalar aplicativos simultaneamente em vários dispositivos ou atualizar arquivos ou drivers em vários dispositivos.

Segurança:

- **LANDesk Antivirus** Instala o agente Antivirus em dispositivos gerenciados. O Antivirus usa o analisador de segurança (instalado com o agente LANDesk padrão) para analisar e identificar vírus em dispositivos gerenciados e fornecer opções para trabalhar com arquivos e pastas infectados. Os administradores descarregam atualizações de definição de vírus e configuram análises de vírus no console do, inclusive a forma como o cliente Antivirus é mostrado nos dispositivos gerenciados e quais opções estão disponíveis ao usuário final. Primeiro você precisa selecionar a caixa de seleção do agente **Antivírus** na página **Iniciar** da Configuração do agente para configurar a página **Antivírus** sob **Segurança**.
- **Segurança de ponto final:** Instala o agente de Segurança de ponto final em dispositivos gerenciados. A Segurança de ponto final protege os seus dispositivos gerenciados de ataques tipo "dia zero" (zero-day), intrusões no firewall e conexões de dispositivos não autorizados. Os serviços de Segurança de ponto final são compostos de três componentes de segurança separados e complementares: HIPS, LANDesk Firewall e Controle de dispositivo.

Inventário e monitoramento em tempo real

Fornece vários métodos para a monitoração do funcionamento de um dispositivo. Enquanto os conjuntos de regras de alerta são definidos no console do Servidor núcleo e distribuídos para vários dispositivos, nos dispositivos individuais você pode definir os contadores de monitoração de desempenho para monitorar questões específicas de desempenho.

- **Componentes de linha básica:** Instala um agente que monitora os hardwares do sistema, como a velocidade do ventilador, o espaço no disco e a temperatura geral do dispositivo.
- **Componentes estendidos:** Instala um agente que monitora o processo do sistema, os serviços e o desempenho geral.

Outras opções:

- **Selecionar todos:** Seleciona todos os agentes disponíveis na lista **Agentes a instalar**.
- **Limpar tudo:** Limpa todos os agentes disponíveis na lista **Agentes a instalar**, com exceção do **agente padrão** do LANDesk, que é obrigatório.
- **Padrões:** Seleciona todos os agentes na lista **Agentes a instalar**, com exceção dos agentes de segurança.
- **Executa uma análise completa de inventário durante a instalação:** Depois da instalação desta configuração faça uma análise completa de inventário. O padrão é selecionado.
- **Mostrar menu iniciar no dispositivo do usuário final:** Quando marcado, cria entradas no menu Iniciar do Windows para os agentes instalados que tiverem uma interface de usuário. Desmarcar essa opção instalará os agentes mas não criará entradas no menu Iniciar.
- **Diretório temporário de instalação:** Especifica a pasta temporária usada nos dispositivos gerenciados durante a instalação. Essa pasta deve ser gravável para a instalação do agente funcionar.

Distribuição do agente LANDesk padrão

Todos os componentes do Management Suite requerem o agente padrão do LANDesk (antes conhecido como CBA), que é instalado por padrão em todas as instalações de dispositivos. Entre outras coisas, o agente LANDesk padrão fornece descoberta de dispositivo e gerencia a comunicação do servidor núcleo/dispositivo.

Como padrão, o agente padrão inclui o analisador de segurança LANDesk Security Suite.

Use as páginas do agente LANDesk padrão para configurar o agente LANDesk padrão, que inclui esses componentes e parâmetros:

- Analisador de inventário
- Agendador local
- Detecção de largura de banda
- Opções de reinicialização de dispositivo

Sobre a página do Agente padrão LANDesk

Use essa página para configurar a segurança baseada em certificado e o escopo que terão os dispositivos que usam essa configuração.

Certificados confiáveis

Selecione os certificados do servidor núcleo que deseja que os dispositivos aceitem. Os dispositivos somente se comunicarão com núcleos e consoles para os quais tiverem certificados. Para obter mais informações sobre certificados e para copiá-los de outros servidores núcleo, para que possam ser selecionados aqui, consulte "Segurança de agente e certificados confiáveis" na página 108.

Abaixo da caixa de certificados confiáveis você pode modificar o servidor núcleo com o qual os dispositivos usando esse agente irão se comunicar. Por padrão, essa caixa contém o servidor núcleo atual. O nome núcleo pode ser o nome de um computador Windows, um endereço IP ou um nome de domínio totalmente qualificado. Pode ser necessário um nome de domínio totalmente qualificado para um núcleo se você estiver enviando configurações de agente a dispositivos em vários domínios ou quando um dispositivo não consegue resolver o nome do núcleo a não ser que seja totalmente qualificado. Os dispositivos gerenciados usarão as informações digitadas para se comunicar com o servidor núcleo; por esta razão o nome aqui digitado deve ser resolvível por todos os dispositivos que receberão esta configuração.

O nome núcleo que você digitar aqui, como parte de uma configuração de agente, é adicionado a um registro de dispositivo sob:

- HKLM\Software\Intel\LANDesk\LDWM\CoreServer

Você poderá testá-los quando os certificados confiáveis forem selecionados - e o nome núcleo tiver sido modificado, se necessário. Quando você clica em **Teste**, uma caixa de mensagem indicando se o nome ou o endereço IP do dispositivo que você digitou é resolvível é exibida. Observe que o botão **Teste** não faz ping ao dispositivo inserido ou verifica se o nome ou endereço IP pertence a um servidor núcleo.

Local (escopo)

Se desejar incluir dispositivos nos escopos baseados em diretórios personalizados, digite um caminho de diretório no campo **Caminho**. O caminho que você digita aqui define o atributo de inventário de local do computador do dispositivo. Os escopos são usados pela administração com base em função da Management Suite para controlar o acesso do usuário aos dispositivos e podem ser baseados neste caminho de diretório personalizado.

Os caminhos de diretório personalizado usam um formato similar a um caminho de arquivo, tendo barras como separadores. Se desejar usar os escopos baseados em diretório personalizado, decida antes como deseja categorizar os seus dispositivos para administração com base em função. Você pode categorizar dispositivos por local geográfico, nome de departamento ou grupo ou por qualquer outro detalhe organizacional que preferir.

Os caminhos de diretório que digitar aqui como parte de uma configuração de agente são adicionados a um registro de dispositivo sob:

- HKLM\Software\Intel\LANDesk\Inventory\ComputerLocation

Não é necessário preencher este campo. Se deixá-lo em branco, o atributo de local do computador do dispositivo é definido pelo seu caminho de Active Directory ou de eDirectory.

Quando o analisador de inventário é executado em um dispositivo, ele registra o atributo local de computador do dispositivo. Se você digitou um caminho de diretório personalizado no campo **Caminho**, esse caminho é o diretório que o analisador grava. Se você deixou vazio o caminho do diretório personalizado, o analisador tentará preencher o atributo de local do computador com o caminho do Active Directory ou do NetWare eDirectory do dispositivo. Se não for encontrado um diretório personalizado e nem um diretório compatível com LDAP, o atributo de local do computador não é definido. Entretanto, o dispositivo, pode ainda ser incluído em escopos de consulta ou escopos de grupo de dispositivo.

Para obter mais informações sobre como os escopos são usados na administração com base em função Management Suite e como você pode definir um escopo usando caminhos de diretório personalizado, consulte "Gerenciamento de usuários" na página 38.

Sobre a página Analisador de inventário (em Agente padrão do LANDesk)

A página do **Analisador de inventário** da Caixa de diálogo **Configuração de agente** contém as seguintes características:

- **Atualização manual:** A lista de softwares usados para excluir títulos durante as análises de software é carregada em cada dispositivo remoto. Sempre que a lista de softwares for alterada no console, ela deverá ser reenviada manualmente para os dispositivos remotos.
- **Atualização automática:** Os dispositivos remotos lêem a lista de softwares do servidor núcleo durante as análises de software. Caso essa opção esteja selecionada, cada dispositivo deverá ter uma unidade mapeada para o diretório ldlogon no servidor núcleo, de modo que possam acessar a lista de softwares. Alterações na lista de softwares são imediatamente disponibilizadas para os dispositivos.
    - **Atualizar usando HTTP:** A partir do Management Suite 8, o analisador de inventário pode usar HTTP para a transferência do arquivo LdAppl3.ini. Isso permite que o analisador ofereça suporte a recursos de Multidifusão dirigida como largura de banda adequada e download de parceiro. O download de parceiro permite aos dispositivos que precisam de atualizações do Ldappl3.ini verificarem no servidor núcleo, a data da versão mais recente; em seguida, eles fazem difusão para os parceiros em sua sub-rede para verificar se um deles tem a atualização em seu cache de multidifusão. Se um parceiro tiver a atualização, a transferência de arquivos ocorrerá na sub-rede local sem gerar tráfego na rede pelos roteadores ou conexões de WAN.

Executar análises de inventário:

- **Análises orientadas por evento:** Configura o agendamento do analisador de inventário no dispositivo gerenciado. Como padrão, a análise é definida para analisar o dispositivo uma vez por dia e informar ao servidor núcleo.
- **Quando o usuário faz login:** Executa o analisador de inventário quando o usuário faz o logon no dispositivo gerenciado.
- **Atraso aleatório máx.:** Especifica um intervalo de horário durante o qual a tarefa pode ser executada. Esse atraso permite que as tarefas que são executadas no login não sejam executadas todas de uma vez, assumindo-se que o intervalo de atraso seja longo o suficiente.
- **Quando o endereço IP muda (mini análise apenas):** O disparo do endereço IP só envia uma mini análise para o servidor núcleo, que torna o inventário muito mais rápido nas mudanças de endereço IP
- **Mudar configurações:** Muda os parâmetros e configura uma agenda local personalizada em hora, dia da semana ou mês, se um usuário está conectado, mudanças no endereço IP e largura de banda disponível da rede. O agendamento padrão é executar uma análise a todo dia com um demora aleatória de até uma hora.

Sobre a página do agendador local (abaixo do agente LANDesk padrão)

O agente do planejador local permite que o Management Suite inicie as tarefas do dispositivo com base em uma hora do dia ou na disponibilidade de largura de banda. O agente do planejador local é mais útil para computadores móveis que nem sempre podem estar na rede ou se conectar à ela por meio de uma conexão dial-up. Por exemplo, você pode usar o planejador local para permitir a distribuição de pacotes no computador móvel apenas quando esses dispositivos estiverem na WAN.

Ao agendar os pacotes de software para distribuição ou ao criar as diretivas do aplicativo, você pode especificar qual largura de banda os pacotes ou as diretivas requerem antes de serem aplicados.

O agendador local executa como um serviço nos dispositivos Windows.

A página do **Planejador local** contém os seguinte recursos:

- **Frequência na qual o agente sonda o registro local para encontrar tarefas:** Frequência com que o agendador local procura tarefas. O padrão é 10 segundos. O intervalo de sondagem que você selecionou é repositório no computador local.
- **Freqüência de detecção de largura de banda:** Com que frequência o agendador local verifica a largura de banda. O padrão é 120 segundos. As verificações da largura de banda ocorrem apenas quando há uma tarefa agendada pendente.

Sobre a página de Alerta (em Agente padrão do LANDesk)

Os conjuntos de regras de alertas definem quais eventos exigem ação imediata ou precisam ser registrados para a sua atenção. Um conjunto de regras contém uma coleção de regras de alertas, cada uma com uma ação de alerta correspondente. Ao definir um conjunto de regras de alerta, você pode distribuí-lo em um ou mais dispositivos para monitorar os itens que são importantes para aquele tipo de dispositivo.

Você pode distribuir um dos conjuntos de regras predefinidos ou pode distribuir conjuntos de regras que você criou dentro da ferramenta de alertas.

A página de Alertas contém os seguinte recursos:

- **Adicionar:** Clique em **Adicionar** para adicionar um conjunto de regras existente na lista de **Conjunto de regras de alertas selecionado**. Os conjuntos de alertas dessa lista serão distribuidos para dispositivos que recebem essa configuração de agente.
- **Remover:** Clique em um conjunto de regras e depois em **Remover** para removê-lo da lista de **Conjunto de regras de alertas selecionado**.

Sobre a página Detecção de largura de banda (em Agente padrão do LANDesk)

O agente de detecção de largura de banda permite a detecção da largura de banda entre os dispositivos e o servidor núcleo. Você pode limitar as ações do Management Suite como a distribuição de software com base na largura de banda disponível. Use essa opção se tiver dispositivos remotos ou dispositivos que se conectam à rede por meio de um link lento.

A página de detecção de largura de banda da caixa de diálogo Configuração de agente contém as seguintes características:

- **Escolher o método de detecção de largura de banda:** Selecione entre usar ICMS ou PDS para a detecção de largura de banda. O ICMP envia solicitações de eco de ICMP de vários tamanhos para o dispositivo remoto e usa o tempo de ida e volta dessas solicitações/respostas de eco para determinar a largura de banda aproximada. O ICMP também distingue entre conexões LAN (alta velocidade) e WAN (lenta, mas não dial-up). No entanto, nem todos os roteadores ou dispositivos suportam as solicitações de eco de ICMP.
  Se sua rede não estiver configurada para permitir solicitações de eco de ICMP, será possível selecionar o PDS. Os testes de largura de banda do PDS não são tão detalhados, mas detectam uma LAN ou uma conexão RAS (geralmente dial-up) de largura de banda baixa. O método PDS só funciona se o serviço PDS estiver sendo executado no servidor de pacote. Esse serviço pode ser instalado através da distribuição do agente LANDesk padrão para o servidor de pacote.

- **Limite da LAN, em bits por segundo:** O limite que classifica uma conexão como WAN em vez de LAN. O padrão é 262.144 bps.

Sobre a página Opções de reinicialização do dispositivo (em Agente padrão do LANDesk)

Assim que você instalar os agentes do Management Suite nos dispositivos, eles podem precisar de reinicialização para concluir a configuração do agente. A página do **Analisador de inventário** da A página de opções para reinicializar o dispositivo contém as seguintes características:

- **Não reinicializar dispositivos após a configuração:** Os dispositivos não serão reinicializados, mesmo se os componentes selecionados requererem uma reinicialização. Se for necessária uma reinicialização, os componentes não funcionarão corretamente até que o dispositivo seja reinicializado.
- **Reinicializar dispositivos se necessário:** Reinicializa os dispositivos somente se um componente selecionado exigir uma reinicialização.
- **Reinicializar com opção do usuário para cancelar:** Se um agente selecionado exigir uma reinicialização, os usuários terão a opção de cancelar a reinicialização. Se for necessária uma reinicialização, os componentes não funcionarão corretamente até que o dispositivo seja reinicializado. É possível definir o tempo que o prompt de reinicialização permanece na tela do usuário antes de o computador ser reinicializado. Esse tempo limite é útil para usuários que estão distantes de seus computadores quando ocorre a distribuição do dispositivo.
- **Permitir ao usuário cancelar a reinicialização dentro deste período:** Se desejar conceder aos usuários a chance de cancelar a reinicialização antes de ela ocorrer automaticamente, digite a duração desejada para o aviso da reinicialização.

Sobre a página Monitoração do uso do software (em Agente padrão do LANDesk)

A página de monitoramento de uso do software é usada para rastrear estatística de uso para Monitoramento de licenças de softwares. Este recurso coleta informações sobre os três tipos de dados: estatísticas de uso da monitoração de licença de software, informações de inventário adicionais e recursos de bloqueio de aplicativo.

Quando agentes distribuídos para imagens de disco interface de desktop (VDI) virtual não persistente, você deve definir um caminho UNC onde os arquivos de dados do monitor de software será armazenado. Se você não definir um caminho, o monitoramento de licença de software armazenará os dados de monitoramento no registro. Em um ambiente não-persistente, estes dados serão perdidos quando a imagem for redefinida. Para obter mais informações, veja "Distribuição de agentes para imagens não-persistentes de VDI" na página 111.

A janela Monitoração do uso de software contém as seguintes opções:

- **Usar monitoramento de software:** Habilita o controle de software através da monitoração de licenciamento de software, análises de inventário e bloqueio de aplicativo através do recurso bloqueador de aplicativos.
- **Grave as estatísticas de uso do software em outro local na rede:** Selecionar isso e configurar as opções relacionadas se vocês estiver distribuindo essa configuração de agente para uma imagem VDI não persistente.
- **Caminho UNC onde os arquivos de monitoramento de dados serão armazenados:** O caminho UNC que você deseja usar está nesse formato: \\servername\sharename.
- **Domínio e nome de usuário:** As credenciais do usuário que permitirão acesso ao caminho UNC.
- **Senha** e **Confirmação de senha:** A senha para a conta de usuário fornecida.

Distribuindo formulários de dados personalizados

Você pode criar e distribuir formulários de dados personalizados para coletar informações sobre o dispositivo que irão complementar as informações padrão disponíveis no banco de dados núcleo. Os formulários criados usando o designer de formulários podem ser distribuídos por um serviço de distribuição de dispositivo ou uso da caixa de diálogo configuração de agente.

Personalize os formulários que são distribuídos aos dispositivos em seu domínio de gerenciamento usando o designer de formulários. Para obter mais informações, consulte "Uso de formulários de dados personalizados" na página 154.

Sobre a página Formulários de dados personalizados

A seção de formulários de dados personalizados consiste em duas páginas. A página de Formulários de dados personalizados contém as seguintes características:

- **Formulários de atualização manual:** Os formulários selecionados são enviados a cada dispositivo. Se os formulários forem modificados ou se novos formulários forem adicionados, eles devem ser reenviados manualmente aos dispositivos remotos.
- **Atualização automática:** Os dispositivos remotos verificam o servidor núcleo para obter formulários atualizados sempre que o analisador de inventário for executado, como na inicialização. Cada dispositivo deve ter uma unidade mapeada para o diretório ldlogon no servidor núcleo para acessar os formulários atualizados.
- **Mostra os formulários ao usuário final:** Definir a forma como os dispositivos remotos acessam os formulários personalizados:
    - **Na inicialização:** Os formulários selecionados são executados automaticamente na inicialização em cada dispositivo.
    - **Quando o analisador de inventário é executado:** Os formulários selecionados são executados somente quando o analisador de inventário é executado em cada dispositivo. O analisador de inventário é executado automaticamente na inicialização e pode ser executada manualmente pelos dispositivos a qualquer momento.
    - **Quando iniciados da pasta de programa do LANDesk:** Os formulários selecionados são mostrados como itens na pasta LANDesk Management do dispositivo. Eles não são executados automaticamente.

Sobre a página Formulários enviados com agente da caixa de diálogo Configuração de agentes

A página Formulários enviados com agente contém todos os formulários de dados personalizados definidos. Selecione quais formulários estarão disponíveis aos dispositivos que estão recebendo essa tarefa de configuração. Será necessário criar os formulários (**Ferramentas > Configuração > Formulários de dados personalizados**) para eles serem exibidos nessa lista.

Instalação da distribuição de software

A distribuição de software automatiza o processo de instalação de aplicativos de software e distribuição de arquivos aos dispositivos. Use esse agente para instalar aplicativos simultaneamente em vários dispositivos ou atualizar arquivos ou drivers em vários dispositivos.

A distribuição de software utiliza um servidor da Web ou de arquivos para armazenar pacotes. Os dispositivos acessam esse servidor de pacotes ao fazer o download de um pacote. Você precisará configurar um pacote de servidor como descrito na seção de distribuição de software. É possível distribuir o agente de distribuição de software para os dispositivos antes de configurar um servidor de pacotes. Para obter mais informações, consulte "Distribuição de softwares/Distribuição de pacotes/Métodos de entrega" na página 258.

Sobre a página Distribuição de software

A página da caixa de diálogo Configuração de agente de Distribuição de software contém as seguintes características:

- **Destino do cliente:** O local onde os aplicativos virtualizados distribuídos são armazenados nos dispositivos gerenciados. Essa opção não tem nenhum efeito se você não está distribuindo aplicativos virtualizados criados com o LANDesk complemento Virtualização do Aplicativo.
- **Habilitar direcionamento de grupo LDAP:** Permite a atribuição de acesso virtual a aplicativos virtuais a OUs ou grupos específicos de um Diretório ativo.

Sobre a página Opções de diretivas (em distribuição de software)

O agente de distribuição baseada em diretiva o capacita a instalar automaticamente conjuntos de aplicativos em grupos de dispositivos. Use esse agente para gerenciar grupos de dispositivos com necessidades de software em comum.

O portal de distribuição de software da LANDesk executa dispositivos gerenciados e mostra softwares disponíveis para aquele dispositivo gerenciado. Para exibir os softwares disponíveis, o portal de distribuição de softwares precisa obter periodicamente informações de diretivas no servidor núcleo. As atualizações de diretivas ocorrem quando:

- Um usuário inicia o portal de distribuição de software da LANDesk a partir do menu Iniciar do Windows.
- Na tela de logon, se a opção execução do logon **LANDesk portal de distribuição do** software for selecionada.
- No logon, se a opção executar no logon a ação de **Atualizar informações de diretivas a partir do núcleo** estiver selecionada.
- No intervalo do agendador local você especifica quando clicar no botão **Mudança de configurações.** Por padrão, os dispositivos gerenciados usam o planejador local uma vez por dia para obter as atualizações de diretivas.

A página de opções de diretivas contém as seguintes características:

- **Quando o usuário fizer logon:** Se selecionado, o dispositivo gerenciado exibe as informações de diretivas depois que o usuário faz logon. O **Atraso aleatório máximo** permite que o usuário atrase a atualização pelo tempo digitado (em horas).
- **Quando o endereço IP mudar:** Se selecionado, o dispositivo gerenciado atualiza as informações de diretiva quando o endereço IP mudar.
- **Mudar configurações:** Usar isso para mudar a frequência e quando o agendador local procurar por atualizador de diretivas. Essa programação é um acréscimo a qualquer opção de execução no logon que você selecionar.

Sobre a página LaunchPad (em distribuição de software)

Use esta página para configurar que personalização de LaunchPad os usuários finais podem fazer. O LaunchPad organiza links para distribuir software nos dispositivos gerenciados. O software distribuído pode ser local, hospedado ou pode ser aplicativos instalados "just-in-time" (no momento necessário). A página LaunchPad contém os seguinte recursos:

- **Permite usuários redimensionar painéis de LaunchPad:** Permite usuários mover e redimensionar os painéis.
- **Permite usuários mover e docar painéis de LaunchPad:** Permite usuários docar painéis em qualquer parte do desktop.

Sobre a página Portal (em distribuição de software)

A página Portal contém todas as tarefas de pacotes de distribuição de software que foram distribuídas usando um método de entrega baseado em diretiva. Use esta página para personalizar a aparência da janela Portal.

Um método de entrega baseado em diretiva se comporta diferente de um envio, ele requer que o dispositivo gerenciado seja iniciado para solicitar diretivas. Isso significa que o pacote não é enviado para o dispositivo do servidor núcleo, mas seus detalhes são armazenados no banco de dados do servidor núcleo até o dispositivo gerenciado consultar o servidor núcleo sobre tarefas de distribuição de software baseadas em diretiva a ele atribuídas. Quando o portal é aberto, ele abre automaticamente a ferramenta de sincronização de diretiva para atualizar sua lista com novas tarefas que foram atribuídas ao dispositivo gerenciado.

A página do Portal contém as colunas opcionais e colunas de exibição e ordem para os campos de Aplicativos. Esses campos são usados para esquematizar as opções de informações adicionais de personalização sobre todos os pacotes na janela Portal de distribuição de software do LANDesk Desktop Manager. A janela Portal de distribuição de software contém as guias Disponível e Histórico que são definidas na página do Portal de configuração de agente. As colunas de campo Opcional possibilitam que você organize as colunas Aplicativo e Histórico que aparecem nas guias e agrupe as informações em uma maneira lógica.

A página Portal contém os seguinte recursos:

- **Aplicativo:** Mostra pacotes atualmente relacionados para distribuição de software iniciada por usuário opcional ou recomendada.
- **História:** Mostra todos os pacotes que foram tentados ou instalados através de diretiva usando o portal.
- **Colunas opcionais:** As colunas que aparecem nas guias **Aplicação** e **Histórico** na janela Portal de distribuição de software do LANDesk Desktop Manager no dispositivo gerenciado.
    - **Tamanho:** Mostra o tamanho físico do pacote de modo a informar o usuário antes de continuar o download de um aplicativo grande.
    - **Grupo:** Permite que os administradores LANDesk especifiquem um grupo em cada tarefa de pacote de distribuição individual a aplicativos que habilitará os usuários finais a classificar a lista de aplicativos por tipo, fornecedor ou categoria, por exemplo. Grupos são atribuídos em cada tarefa individual de distribuição de software agendada.
    - **Descrição:** Mostra a descrição de propriedades do pacote de distribuição.
    - **Status:** Indica se a instalação foi bem-sucedida ou falhou.
    - **Última execução:** Indica a data e a hora da última tentativa para instalar o pacote.
    - **Tipo:** Indica se o pacote é requerido, recomendado ou opcional.

- **Mostra colunas e a ordem para o aplicativo/histórico:** Mostra as colunas padrão nas guias Aplicação e Histórico na janela Portal de distribuição de software do LANDesk Desktop Manager no dispositivo gerenciado. A lista padrão contém o seguinte:
  - **Nome (requerido):** Mostra o nome do pacote de distribuição.
  - **Descrição** (opcional)
  - **Status** (opcional)
  - **Última execução** (opcional)
  - **Tipo** (opcional)
  - Use os botões **Para cima** e **Para baixo** para reorganizar a ordem na qual a coluna aparece.

Distribuição do controle remoto

Durante a distribuição do controle remoto, é preciso considerar qual modelo de segurança deseja utilizar. As opções são as seguintes:

- **Modelo local:** Esta é a segurança mais básica que utiliza quaisquer configurações de controle remoto que estiverem especificadas no dispositivo. Este modelo não requer nenhuma outra autenticação ou participação em grupo.
- **Modelo de segurança/local do Windows NT:** Este modelo de segurança usa um grupo de Operadores de controle remoto do Windows NT. Os membros desse grupo têm permissão para controlar dispositivos remotamente. O usuários permitidos ainda usam as configurações de controle remoto do dispositivo, essa permissão é requerida.
- **Segurança integrada:** Esta é a opção mais segura e é o padrão. Segurança integrada é descrita na seção a seguir.

Sobre a Segurança integrada

A segurança integrada é o novo modelo de segurança padrão. A seguir, há uma descrição do fluxo de comunicação do controle remoto de segurança integrada:

1. O usuário do controle remoto se conecta ao agente do controle remoto do dispositivo gerenciado, mas o agente responde que é necessária uma autenticação de segurança integrada.
2. O usuário pede direitos de controle remoto do servidor núcleo.
3. O servidor núcleo calcula os direitos de controle remoto baseado no escopo do usuário, direitos de administração com base em funções e direitos do Active Directory. O servidor núcleo, então, cria um documento assinado e seguro e o devolve ao usuário.
4. O usuário envia esse documento ao agente de controle remoto no dispositivo gerenciado, o qual verifica o documento assinado. Se tudo estiver correto, o agente permite o início do controle remoto.

AVISO: A segurança integrada requer o servidor núcleo
No controle remoto de segurança integrada, se o servidor núcleo não estiver disponível, os consoles não poderão controlar os dispositivos remotamente. O controle remoto de segurança integrada exige que o servidor núcleo funcione.

Uso da segurança/modelo local do Windows NT com dispositivos Windows XP

Para que a autenticação de segurança/modelo local do Windows NT funcione com dispositivos Windows XP, você deve configurar os dispositivos de forma que o modelo de compartilhamento e segurança do Windows XP para contas locais seja o clássico (os usuários locais se autenticam como eles mesmos). Se isso não for feito, a autenticação padrão apenas como convidado não funcionará com a segurança do Windows NT do controle remoto.

Para definir o modelo de segurança do Windows XP como clássico

1. No dispositivo Windows XP, clique em **Iniciar > Painel de controle**.
2. No miniaplicativo **Ferramentas administrativas > Diretiva de segurança local**, clique em **Opções de segurança >Acesso à rede: Modelo de compartilhamento e segurança de contas locais**, e defina como **Clássico - usuários locais autenticam-se como eles mesmos**.

Sobre a página Controle remoto

Usar a página de Controle remoto para selecionar e configurar perfis de configurações de controle remoto. Você também, pode mudar as configuraçõesda unidade aqui.

- **Escolha quais configurações do controle remoto aplicar:** Exibi a lista de perfis de configurações de controle remoto que estão disponíveis. Você pode selecionar o perfil que quiser que essa configuração de agente use..
- **Configurar:** Abre a caixa de diálogo de Configurações do controle remoto, onde você pode configurar e gerenciar os perfis de configuração do controle remoto.
- **Usar mirror driver:** Selecionada por padrão, esta opção usa o mirror driver do controle remoto nos dispositivos para um desempenho remoto mais rápido.
- **Usar driver de tela em branco:** Selecionada por padrão, esta opção usa um driver especial que pode dizer ao driver de vídeo do dispositivo alvo para desligar o monitor. Quando ativo, esse driver filtra os comandos e usa o driver de vídeo real para impedir que liguem o monitor. Os operadores de controle remoto podem ligar ou desligar a tela em branco do aplicativo do usuário de controle remoto. Se tiver problemas de compatibilidade com esse driver, poderá desmarcar a caixa de seleção para usar um modo de tela em branco mais compatível - porém possivelmente menos eficaz. Se você não usar o driver de tela em branco, o modo alternativo pode provocar oscilações na tela do dispositivo alvo durante o controle remoto. Essa opção requer o mirror driver.

Sobre a caixa de diálogo Configurações de controle remoto

Usar a caixa de diálogo Configurar controle remoto para gerenciar suas configurações de perfis de controle remoto. Você pode criar configurações múltiplas de perfis de controle remoto e selecionar aquele que você quer que seja padrão para as configurações.

- **Novo:** Criar um novo perfil de configurações para um novo controle remoto.
- **Editar:** Edita um perfil existente.
- **Copiar:** Abre um arquivo selecionado e insere "Copiar em" no início do **Nome** do perfil selecionado. Quando clicar em **Salvar**, ele será salvo como um novo perfil.
- **Excluir:** Exclui o perfil selecionado. Você terá que confirmar a exclusão.
- **Usar selecionada:** Fecha a caixa de diálogo de Configurações do controle remoto e faz do perfil que você selecionou no **Escolher em qual configuração do controle remoto aplicar** a caixa de listas suspensa.

Sobre a página Configurações gerais

A página da caixa de diálogo Configuração de agente de Controle remoto contém as seguintes características:

- **Modelo local:** Usa apenas as permissões simples de dispositivo local definidas na página **Permissões** do controle remoto.
- **Segurança / modelo local do Windows NT:** Permite que apenas membros do grupo Operadores do controle remoto iniciem conexões do controle remoto a do console para dispositivos remotos. Os usuários com permissão ainda precisam utilizar as permissões definidas na página de Configurações do controle remoto desta caixa de diálogo.
  Como o grupo Operadores do controle remoto é um grupo local, cada dispositivo tem sua própria cópia do grupo. Para evitar o gerenciamento individual de cada grupo de Operadores do controle remoto do dispositivo, inclua grupos globais (a nível de domínio) em cada grupo local.
  O usuários permitidos ainda usam as configurações de controle remoto do dispositivo, essa permissão é requerida.
- **Segurança integrada:** Esse é um modelo de segurança padrão e descrito anteriormente nesta seção. Os usuários permitidos ainda precisam usar o conjunto de permissões na **página Permissões**.
- **Permitir acesso HTML:** Permite que agente controle remoto receba solicitações de controle remoto HTML. Para obter mais informações, consulte Controle remoto HTML.
- **Definir como padrão:** Faz o perfil de configuração do controle remoto que você está configurando o padrão de configurações do controle remoto para novas configuração de novo agente.

Adição de usuários ao Grupo de operadores do controle remoto e Grupo apenas ver

Se selecionar **Segurança do Windows NT/modelo local** como seu modelo de segurança, as caixas **Grupo de operadores do controle remoto** e **Grupo Apenas ver** mostram os usuários para o console ou para o domínio do Windows NT selecionado. Os usuários selecionados aqui terão acesso ao controle remoto dos dispositivos que recebem as configurações definidas neste arquivo de configurações. **Grupo apenas ver** os usuários só podem ver dispositivos remotos. Eles não podem assumir controle do mouse ou do teclado.

Ao adicionar usuários a um dos grupos de controle remoto, o console utiliza as credenciais do Windows do usuário conectado e não as credenciais dos usuários do console da LANDesk para mostrar os usuários de um domínio. Se a caixa **Listar usuários de** não mostrar o domínio que deseja, conecte-se no Windows como usuário com direitos para aquele domínio.

Para escolher entre um servidor ou um domínio existente

1. Na página **Controle remoto**, clique em **Segurança do Windows NT/modelo local** e clique no botão **Adicionar**.
2. Na caixa de **Listas de usuários**, selecionar o nome do servidor núcleo ou nome de domínio Windows NT contendo os Usuário das contas.
3. Na lista de usuários, selecione um ou mais usuários e clique em **Inserir** para adicioná-los à lista de **Nomes inseridos**.
4. Clique em **OK** para adicionar os nomes selecionados ao grupo de Operadores do controle remoto em cada dispositivo que recebe essas configurações.
5. Se desejar que alguns desses usuários estejam no **Grupo apenas ver**, selecione-os e mude-os. Os usuários só podem estar em um grupo.

Para inserir nomes manualmente

Você pode inserir nomes manualmente clicando na lista **Nomes inseridos** e usando um dos seguintes formatos para inserir nomes. Use ponto-e-vírgula para separar os nomes.

- **DOMAIN\nome do usuário** onde DOMAIN é o nome de qualquer domínio acessível ao dispositivo alvo.
- **MACHINE\nome do usuário** onde MACHINE é o nome de qualquer dispositivo no mesmo domínio que o dispositivo alvo.
- **DOMAIN\nome do grupo** onde DOMAIN é o nome de qualquer domínio acessível ao dispositivo alvo e o nome do grupo é o nome de um grupo de gerenciamento naquele domínio.
- **MACHINE\nome do grupo** em que MACHINE é o nome de qualquer dispositivo no mesmo domínio que o nó gerenciado e o nome do grupo é o nome de um grupo de gerenciamento naquele dispositivo.

Se você não especificar um domínio ou um nome de dispositivo, supõe-se que esse usuário ou grupo especificado pertença ao dispositivo local.

Clique em **OK** para adicionar os nomes ao grupo de usuários Operadores do controle remoto no dispositivo alvo.

Sobre a página Indicadores (em Controle remoto)

A página de indicadores da seção do Controle remoto contém as seguintes características:

- **Ícone flutuante no desktop:** Exibe o ícone do Agente do controle remoto na tela do dispositivo todas as vezes ou apenas quando está sendo controlado remotamente. Quando está sendo controlado pelo console, o ícone torna-se uma lente de aumento e a barra de título do ícone fica vermelha.
- **Ícone da bandeja do sistema:** coloca o ícone do Agente do controle remoto na bandeja do sistema. Mais uma vez, o ícone pode ser visível sempre ou apenas enquanto estiver sendo controlado remotamente.
- **Bloquear o computador controlado remotamente quando a sessão terminar:** Bloqueia o dispositivo gerenciado no modo protegido esteja o usuário conectado ou não.

Sobre a página Permissões (em controle remoto)

A página **Permissões** da seção**Controle remoto** contém os seguintes recursos:

- **Controle remoto:** Concede permissão para controlar o dispositivo.
- **Desenhar:** Concede permissão para usar as ferramentas de desenha janela do visor no dispositivo.
- **Apenas ver:** Os operadores de controle remoto só podem ver o dispositivo, não podem interagir com o mesmo remotamente.
- **Chat:** Concede permissão para bate-papo com o dispositivo.
- **Transferência de arquivos:** Concede permissão para transferir arquivos de e para as unidades locais do dispositivo.
- **Executa programas no dispositivo remoto:** Concede permissão para executar programas no dispositivo.
- Executar como administrador: Executar programas sob administrador de contas.
- **Reinicializar:** Concede permissão para reinicializar o dispositivo.

- **Especificar as configurações de controle remoto:** Configura e define permissões para usuários do Controle remoto. Mensagens personalizadas podem ser criadas ao solicitar permissões para executar os diferentes comandos que o controle remoto oferece.
    - **Fechar sessão inativa após:** Permite à sessão remota desconectar automaticamente por inatividade. Se for inserido o valor 0, o console não desconectará automaticamente a sessão remota por inatividade.
    - **O usuário final precisa conceder permissão para a sessão de controle remoto:** Permite a um usuário que acessou um dispositivo gerenciado controlado remotamente responder afirmativamente à solicitação antes que o controle desse dispositivo seja assumido.
    - **Somente quando o usuário estiver conectado:** Solicita a permissão do usuário conectado no momento. Se não houver ninguém conectado, o controle remoto não requer permissão.
    - **Pedir permissão para todos os recursos de uma vez:** Permite a solicitação de permissões uma vez por sessão em vez de solicitar permissão para cada recurso (transferência de arquivo, executar remoto, etc.) Se esta caixa de seleção estiver selecionada, a permissão será solicitada ao usuário somente uma vez durante a sessão de controle remoto, independentemente dos processos executados.
    - **Mostra uma mensagem personalizada:** Mostra ao usuário uma mensagem personalizada solicitando permissão para executar uma das seguintes ações:
        - Controle remoto
        - Bate-papo
        - Execução remota
        - Transferência de arquivos
        - Reinicializar
        - Todas as permissões
    - **Fechar a caixa de mensagem de permissão após:** Permite ao usuário aceitar ou recusar permissão (em segundos) ao dispositivo gerenciado. Esta é uma definição configurável de tempo de duração da janela de permissão ao solicitar permissão para controlar remotamente um dispositivo gerenciado.

Distribuindo serviços de Segurança LANDesk

O analisador de segurança (analisador patch e conformidade) é instalado como padrão com o agente LANDesk padrão. Entretanto, você precisa usar as opções na página específica de análise de security e patch ao criar configurações de agentes de dispositivos para configurar determinados aspectos sobre como e quando a análise de segurança será executada em dispositivos gerenciados. Você também pode ativar e configurar definições personalizadas de desvios das variáveis, freqüentes análises de segurança, spyware em tempo real e bloqueamento de aplicativos.

A análise de segurança permite analisar dispositivos por SO conhecidos e vulnerabilidade de aplicativos e riscos de segurança como, spyware, aplicativos não autorizados, atualizações de software e drivers, ameaças de segurança de configuração de sistema, definições de segurança personalizadas e outras. O conteúdo da sua análise de segurança depende da sua assinatura de conteúdo do Security Suite e das definições de tipo de segurança que você descarregou. Você também pode corrigir problemas detectados através de correções automáticas e diretivas de reparo. Para obter mais detalhes sobre esses procedimentos, consulte "Patch e conformidade" na página 549.

Informações sobre as páginas relacionadas à segurança a seguir podem ser encontradas abaixo. Clique em um link para ir para a seção correspondente.

- "Sobre a página Análise de Patch e conformidade" na página 127
- "Sobre a página Variáveis personalizadas" na página 128
- "Sobre a página Análise de segurança frequente" na página 129
- "Sobre a página LANDesk Antivirus" na página 129
- "Sobre a página Spyware" na página 130
- "Sobre a página Bloqueador de aplicativo" na página 131
- "Sobre a página Firewall do Windows" na página 131
- "Sobre a página Segurança de ponto final" na página 132
- "Sobre a página do Agent Watcher" na página 132
- "Sobre página de suporte LANDesk 802.1x" na página 132
- "Sobre a página Descoberta estendida de dispositivos" na página 135

Sobre a página Análise de Patch e conformidade

Use esta página para configurar como a análise de segurança (isto é, analisador de correção e conformidade) será iniciada e como se comporta em dispositivos gerenciados com esta configuração de agente.

NOTA: É possível também realizar análises de segurança como tarefas agendadas e diretivas do console ou manualmente no dispositivo.

Essa página contém as seguintes opções:

- **Análise orientada por evento:**
  - **Quando o usuário faz login:** Coloca a análise de segurança na chave de execução do registro do Windows, fazendo com que a análise inicie sempre que ocorrer um login nos dispositivos gerenciados com esta configuração de agente.
- **Análise orientada por agendamento:**
  - **Mudar configurações:** Abrir a caixa de diálogo **Agendar análise de segurança e patch**, onde você pode configurar agendamentos para análises de segurança que são iniciadas pelo agendador local. O agendador local automaticamente lança uma análise de segurança repetidamente, o mais cedo dentro de um período de tempo e restrições que você especificar. É também possível configurar opções para executar o analisador de segurança quando um dispositivo satisfaz determinadas condições, por exemplo: somente quando um usuário está conectado, somente se uma largura de banda mínima especificada estiver disponível e em qualquer hora em que o endereço IP do dispositivo mudar. Quando você tiver configurado essas definições de agendamento para o analisador de segurança, simplesmente clique em **Salvar** para voltar à página principal onde agora é exibido o critério de agendamento.

- **Configurações globais:** aplica-se a todos os dispositivos com esta configuração de agente, cancelando as configurações específicas as tarefas.
    - **Nunca reinicializar:** assegura que os dispositivos com essa configuração de agente não reinicializem quando o analisador de segurança estiver em execução. Este é um parâmetro global para todos os dispositivos com essa configuração de agente, o que significa que ele sobrescreve quaisquer configurações de reinicialização do usuário final aplicadas à análise de segurança ou a uma tarefa de reparo. Em outras palavras, independente das configurações de reinicialização do usuário final usadas por uma tarefa de segurança, esse parâmetro global terá precedência. Selecione esta opção se não desejar que os dispositivos reinicializem durante uma operação de análise de segurança e de correção, e mantenha desmarcada se desejar configurar as opções de reinicialização com a ferramenta Segurança e Conformidade (Security and Compliance).
    - **Nunca fazer reparo automático:** Assegura que os dispositivos com essa configuração de agente não permitam que a análise de segurança e patch faça correção automática ao remediar vulnerabilidades detectadas, mesmo se a vulnerabilidade tiver a correção automática ativada. Por ser um parâmetro global para todos os dispositivos com essa configuração de agente, essa configuração substitui qualquer parâmetro de reparo automático que o usuário final aplicar à tarefa de análise de segurança. Use esta configuração se desejar garantir que as vulnerabilidades detectadas dos dispositivos não sejam remediadas automaticamente por uma análise de segurança.
- **Configurações de análise e reparo:** Determina a informação exibida pelo verificador de segurança em dispositivos gerenciados, interação com usuário final, operação reinicializar, e configurações de conteúdo quando o analisador é lançado em dispositivo gerenciado com essa configuração de agente pelo método selecionado acima (executa chave durante o acesso, agendador local, ou ambos). Selecione uma configuração de análise e reparo na lista suspensa para aplicá-la à configuração que está criando. Se desejar, clique em **Configurar** para criar e aplicar uma nova configuração de análise e reparo ou para editar uma já existente.

Sobre a página Variáveis personalizadas

Use esta página para designar uma definição de desvios das variáveis personalizadas com essa configuração de agente.

O analisador de segurança pode utilizar variáveis personalizadas (valores editáveis incluídos em certas definições de tipos de segurança) para analisar e modificar definições específicas e para implementar definições padrão do sistema nos dispositivos gerenciados. É possível mudar o valor de uma definição e selecionar se deseja sobrescrever o valor atual com o novo valor e depois usar essa configuração de agente para aplicar a configuração nos dispositivos gerenciados. Em algumas situações, talvez você deseje ignorar uma definição de variável personalizada, ou, em outras palavras, criar uma exceção à regra. As configurações para substituir as variáveis personalizadas permitem decidir quais variáveis deverão ser ignoradas ao analisar dispositivos para que eles não sejam detectados como vulneráveis e corrigidos mesmo que atendam às condições de regras de detecção de uma definição.

Uma definição de desvio da variável personalizada não é necessária com uma configuração de agente.

Você pode selecionar uma Configuração existente pela lista **Configurar variáveis personalizadas**, clique em **Configurar** para criar uma nova configuração, ou deixe o campo em branco.

Essa página contém as seguintes opções:

- **Definições das variáveis personalizadas:** Especifica as definições de sobrescrição das variáveis personalizadas em dispositivos quando são analisados por definições de segurança que incluem

variáveis personalizadas (como, por exemplo, ameaças de segurança e vírus). As configurações de substituição de variáveis personalizadas permitem especificar os valores definidos que você deseja ignorar durante uma análise de segurança. Isso é muito útil em situações em que você não deseja que um dispositivo analisado seja identificado como vulnerável de acordo com as configurações de variáveis personalizadas padrão de uma definição. Selecione uma configuração da lista. A partir da lista , você também pode remover configurações de substituição de variáveis personalizadas dos dispositivos alvo. A opção **Remover definições das variáveis personalizadas** permite limpar um dispositivo para que as definições de variável personalizada funcionem completamente. Clique em **Editar** para modificar as opções da configuração selecionada. Clique em **Configurar** para criar uma nova definição. Para obter mais informações, consulte "Sobre a caixa de diálogo Configurar as definições da variável personalizada a ser substituída" na página 650.

Sobre a página Análise de segurança frequente

Use esta página para ativar e configurar uma análise recorrente de segurança para uma coleção específica de vulnerabilidades com alto risco ou outras definições de segurança nos dispositivos com essa configuração de agente. Uma análise frequente de segurança é útil se você precisar analisar dispositivos regularmente para ataques de segurança particularmente agressivos ou danosos.

NOTA: Somente análises de grupo
Análises de segurança frequentes são baseadas em definições de segurança contidas em um grupo que você selecionou nos grupos de conteúdo de segurança pré-definidos.

Essa página contém as seguintes opções:

- **Usar o analisador freqüente de segurança:** Ativa uma análise freqüente de segurança nos dispositivos com essa configuração de agente.
- **Analisar apenas quando houver um usuário conectado:** Restringe a análise de segurança freqüente para que execute somente se um usuário estiver conectado ao dispositivo alvo.
- **A cada:** especifica o intervalo de tempo para uma análise de segurança freqüente.
- **Escolher um parâmetro de análise e reparo:** Especifica as configurações de análise e reparo que controlam o analisador de segurança para análises freqüentes. As configurações de análise e reparo determinam se a análise de segurança são exibidas em dispositivos durante a execução, opções de reinicialização e interação do usuário. A definição selecionada deve ser configurada para analisar um grupo e não um tipo. Se desejar, clique em **Configurar** para criar uma nova configuração de análise e reparo associada a um grupo.

Sobre a página LANDesk Antivirus

Use esta página para selecionar a configuração de antivírus aplicável aos dispositivos com esta configuração de agente e para selecionar se deseja remover produtos existentes de antivírus dos dispositivos, quando forem configurados.

NOTA: Essa página NÃO se aplica ao novo padrão de configuração de agente Windows Embedded.

Para selecionar uma configuração antivírus, você deve primeiro selecionar a caixa de seleção do agente LANDesk Antivirus na página Início.

As configurações de antivírus permitem controlar como a análise antivírus funciona nos dispositivos alvo. Você pode definir parâmetros de análise antivírus como, por exemplo arquivos e pastas para análise ou exclusão, análises manuais, análises em tempo real, análises agendadas, opções de quarentena e backup, opções de atualização de arquivo de padrão de vírus e informações e opções interativas mostradas nos dispositivos do usuário final durante a análise antivírus.

NOTA: A distribuição do Antivírus do LANDesk para dispositivos que já tiverem um produto de antivírus instalado
Se outro produto de antivírus for instalado nos dispositivos alvo, é possível selecionar a remoção automática durante a configuração de agente através da opção **Remover produto existente de antivírus**. Se escolher a não remoção de outro produto de antivírus durante a configuração de agente, o LANDesk Antivírus é desabilitado até que você remova manualmente o outro produto. Entretanto, você ainda poderá distribuir o agente LANDesk Antivirus a dispositivos alvo.

Para ver a lista atual dos produtos antivírus que podem ser removidos dos dispositivos consulte "LANDesk Antivirus" na página 712.

Essa página contém as seguintes opções:

- **Remover produto existente de antivírus:** Remove automaticamente outro software antivírus que possa já estar instalado nos dispositivos antes da instalação do LANDesk Antivirus. (**NOTA:** Também é possível selecionar a remoção de software de antivírus existente dos dispositivos gerenciados durante a criação de uma tarefa de **Instalação ou atualização do Antivírus**.
- **Definições do LANDesk Antivirus:** Configurações de antivírus determinam se o ícone Antivírus aparece na bandeja do sistema do dispositivo, disponibilidade de opções interativas para usuários finais, verificação de e-mail e ativação de proteção em tempo real, tipos de arquivos para verificar, arquivos e pastas para excluir, quarentena de arquivo infectado e Backup, verificação agendada de antivírus, e definições de atualizações de vírus agendados. Selecione uma configuração da lista. Clique em **Configurar** para criar uma nova definição.

Sobre a página Spyware

Use esta página para habilitar a detecção de spyware em tempo real e notificação em dispositivos com esta configuração de agente.

A detecção de spyware em tempo real verifica somente as definições que residam no grupo de **Análise** e que tiverem a correção automática ligada. Você pode manualmente habilitar a opção de correção automática para definições de spyware carregadas ou configurar atualizações de definição de spyware para que a opção de correção automática seja automaticamente habilitada quando forem carregadas.

A detecção de spyware em tempo real monitora dispositivos para verificar processos iniciados recentemente que tentam modificar o registro local. Se o spyware for detectado, a análise de segurança no dispositivo avisa o usuário final para removê-lo.

Essa página contém as seguintes opções:

- **Permite bloqueamento de spyware em tempo real:** Ativa a monitoração e o bloqueamento de spyware em tempo real nos dispositivos com essa configuração de agente.

  NOTA: Para a análise e detecção de spyware em tempo real funcionar, é necessário habilitar manualmente o recurso de correção automática (autofix) para qualquer definição de spyware descarregada que quiser incluir em uma análise de segurança. As definições de spyware obtidas por

download não vêm com o autofix habilitado como padrão.

- **Notificar o usuário quando o spyware for bloqueado:** Exibe uma mensagem que informa o usuário final sobre a detecção e reparo de um programa spyware.
- **Se um aplicativo não for reconhecido como spyware, peça aprovação ao usuário antes de ser instalado:** Mesmo se o processo detectado não for reconhecido como spyware de acordo com a lista atual de definições de spyware do dispositivo, o usuário final será avisado antes que o software seja instalado no computador.

Sobre a página Bloqueador de aplicativo

Use esta página para habilitar bloqueamento e notificação de aplicativos não autorizados em tempo real. O bloqueador de aplicativos em tempo real verifica somente os aplicativos que residem no grupo Análise.

Para o bloqueamento de aplicativos em tempo real, a correção NÃO é uma tarefa separada. O bloqueio de aplicativos ocorre como parte da própria análise de segurança, com a edição do registro no disco rígido local para desativar o acesso do usuário aos aplicativos não autorizados. Os serviços de segurança utilizam o recurso softmon.exe da ferramenta de monitoração de licença para negar o acesso a executáveis de aplicativos especificados mesmo se o nome de arquivo do executável tiver sido modificado porque o softmon.exe lê as informações do cabeçalho do arquivo.

Essa página contém as seguintes opções:

- **Permitir bloqueamento de aplicativos não autorizados:** Ativa o bloqueamento de aplicativos em tempo real nos dispositivos com essa configuração de agente.
- **Notificar o usuário quando um aplicativo for bloqueado:** Mostra uma mensagem ao usuário final notificando-o que tentaram iniciar um aplicativo não autorizado e o acesso foi negado.

Sobre a página Firewall do Windows

Use esta página para habilitar e configurar o firewall do Windows nos dispositivos gerenciados com esta configuração de agente. Você pode habilitar/desabilitar o firewall e configurar definições de firewall incluindo exceções, regras de entrada e de saída (para serviços, portas, programas).

É possível usar esse recurso para distribuir uma configuração para o firewall Windows nas seguintes versões do Windows:

- Windows 2003
- Windows XP (SP2 ou mais recente)
- Windows Vista

Essa página contém as seguintes opções:

- **Configurar firewall do Windows:** Habilita a configuração automática do Windows em dispositivos com essa configuração de agente.
- **Configurações do Firewall do Windows:** Especifica as configurações de firewall do Windows distribuídas para dispositivos alvos com essa configuração de agente. Selecione uma configuração da lista disponível para aplicá-la à configuração do agente que está sendo criado. Se desejar, clique em **Configurar** para criar e aplicar uma nova configuração de análise e reparo ou para editar uma já existente.

Sobre a página Segurança de ponto final

Use esta página para selecionar uma configuração do Segurança de ponto final para dispositivos gerenciados com esta configuração de agente. A Segurança de ponto final inclui os seguintes componentes: HIPS, LANDesk Firewall e Controle de dispositivo.

Para selecionar uma configuração de Segurança de ponto final, é preciso primeiro marcar a caixa de seleção Segurança de ponto final de agente, na página **Iniciar**.

Essa página contém as seguintes opções:

- **Configurações de Segurança de ponto final:** Especifica as definições de Segurança de ponto final para dispositivos gerenciados com essa configuração de agente. As configurações de Segurança de ponto final determinam a operação geral da Segurança de ponto final (como alerta para local, senha de administrador, opção de parada de usuário final e mensagens de pop-up), além de determinar que diretivas de segurança são distribuídas por HIPS, LANDesk Firewall e Controle de dispositivo. Clique também em **Configurar** para criar novas definições.
- **Atualizar configuração do núcleo:** Permite atualizar as configurações de Segurança de ponto final nos dispositivos configurados com esta configuração de agente.

Sobre a página do Agent Watcher

Use esta página para ativar e configurar o utilitário LANDesk Agent Watcher nos dispositivos com esta configuração de agente.

O Agent Watcher permite monitorar ativamente os dispositivos de LANDesk arquivos e serviços de agente selecionados. O Agent Watcher reinicia serviços de agente que foram interrompidos e reconfigura os tipos de reinicialização nos serviços definidos como automáticos. O utilitário também remove arquivos de agente monitorados das listas de arquivos a serem excluídos na reinicialização, para impedir a exclusão. Além disso, o Agent Watcher o alerta quando os serviços de agente não podem ser reiniciados, quando os arquivos de agente são excluídos e quando os arquivos de agente são agendados para exclusão na reinicialização.

Essa página contém as seguintes opções:

- **Uso do Agent Watcher:** Ativa o utilitário Agent Watcher nos dispositivos com essa configuração de agente.
- **Configurações do Agent Watcher:** Especifica as definições do Agent Watcher distribuídas aos dispositivos alvo com essa configuração de agente. As definições do Agent Watcher determinam quais serviços e arquivos são monitorados e a respectiva freqüência, e se o utilitário permanece residente no dispositivo. Selecione uma configuração da lista. Clique em **Configurar** para criar uma nova definição.

Sobre página de suporte LANDesk 802.1x

Use esta página para ativar a solução LANDesk 802.1x NAC. Você pode usar o 802.1x para reforçar sua diretiva de segurança de conformidade em dispositivos gerenciados compatível com o 802.1x, pela execução de análises de segurança, garantindo ou bloqueando acesso dependendo do status de saúde dos dispositivos (em conformidade), colocando em quarentena dispositivos sem conformidade e executando correções.

NOTA: Habilitação e configuração de 802.1x NAC com uma configuração de agente
Para ativar o 802.1x NAC e configurar as opções nessa página você precisa primeiro selecionar a opção **Servidor Radius 802.1x** na caixa de diálogo Configuração de 802.1x na ferramenta Controle de acesso

de redes (**Ferramentas > Segurança > Controle de acesso de redes > Configurar 802.1x > Servidor Radius**). Após selecionar essa opção você pode usar esta página para configurar 802.1x com uma configuração de agentes.

Essa página contém as seguintes opções:

- **Habilitar suporte ao 802.1x do LANDesk:** Ativa o 802.1x NAC nos dispositivos com essa configuração de agente. O 802.xX NAC usar tipo EAP especificado na ferramenta NAC. A opção de tipo de EAP é válida no núcleo inteiro. Em outras palavras, todos os dispositivos com esta configuração de agente serão definidos com o tipo de EAP especificado no console.
- **Configurar definições PEAP:** Abre a caixa de diálogo onde você pode especificar as configurações do servidor e de autoridade de certificação confiável.
- **Endereço de rede de quarentena:**
  - **Use IP em intervalo auto-atribuído:** Especifica que dispositivos que não estejam em conformidade com base na diretiva de segurança de conformidade serão enviados para a área de quarentena da rede, usando uma função embutida de intervalo de endereço IP auto-atribuído do protocolo de TCP/IP.
  - **Use DHCP na rede de quarentena:** Especifica que os dispositivos que não estiverem funcionando corretamente (não conformidade), com base na diretiva de segurança de conformidade, serão enviados para a área de quarentena da rede usando um servidor DHCP e o servidor de correção que você configurou na rede LANDesk.
    - **Selecionar servidor de correção primário:** Especifica o servidor de correção que você deseja usar para reparar dispositivos sem conformidade, para que possam passar por nova análise e depois possam acessar a rede corporativa.
    - **Servidor de correção de backup:** Permite a você configurar um servidor de backup para correção em caso de a correção primária não puder ser acessada. Clique em **Configurar** para adicionar um servidor de correção.
- **Cliente de quarentena se nenhuma análise de conformidade foi executada em:** Use essa opção para automatizar a quarentena de dispositivos especificando o período máximo de tempo que um dispositivo pode ser considerado em conformidade sem passar por uma análise de segurança de conformidade. Se esse tempo expirar sem uma análise, o dispositivo será automaticamente colocado na área de quarentena da rede.

Distribuindo o filtro escritura para dispositivos Windows Embedded Standard.

Usar essa opção para permitir que um período de tempo específico durante o qual LANDesk Administrator e/ou tarefas agendadas e diretivas criadas pelo administrador pode "escrever" para um dispositivo gerenciado executando Windows Embedded Standard OS.

IMPORTANTE: Somente para dispositivos HP Thin Client WES
Essa opção é disponível somente para HP Thin Client Windows Embedded Standard (WES 7 e WES 09) dispositivos de sistema operacional.

A janela Filtro de gravação incorporado OS é o período de tempo durante o qual o dispositivo gerenciado irá permitir escrever em seu disco rígido. No início dessa "janela de manutenção" o filtro de gravação é desabilitado e o dispositivo reiniciado. Depois aplicadas as diretivas, tarefas, e processos são executados no dispositivo Isso pode levar um tempo curto de um período estendido dependendo das diretivas designadas. Quando as diretivas e processos estiverem concluídos (ou, se a hora de término foi especificada, quando a hora do término da "janela de manutenção" for alcançada) o filtro de gravação (enhanced ou baseado em arquivo) é reativado e o dispositivo reiniciado.

Você pode permitir um período de tempo aberto para permitir que todas as diretivas e processos para completar OU você pode especificar uma hora de término em particular quando operações atuais param e o dispositivo automaticamente reinicia independentemente se o processo está sendo executado ou não. A opção hora de término é uma medida de segurança e de precaução para que o dispositivo não seja exposto a um processo sem garantia por um período estendido de tempo. Entretanto, você deve achar o equilíbrio apropriado de tempo durante o qual são necessárias que as diretivas possam ser completas sem comprometer o status ou funcionamento do dispositivo gerenciado.

CUIDADO: Se você definir uma hora de término específico para o filtro de gravação ser habilitado e para diretivas e processos serem executados e todos os processos incompletos até esse tempo, lembre-se que perda de dados ou corrupção podem ocorrer. Portanto, você precisa medir com exatidão e determinar a quantidade de tempo solicitado para completar todas as diretivas aplicadas e tarefas. Ou, então NÃo defina uma hora de término.

Sobre a página de gravação Embedded OS

Essa página contém as seguintes opções:

- **Janela:** Indica a janela de tempo durante na qual o dispositivo-alvo pode ser escrito.
- **Hora inicial:** Especifica o tempo exato quando a escritura no dispositivo pode começar.
- **Dias da semana habilitado:** Especifica os dias da semana quando as escritura pode acorrer.
- **Especifique uma hora de término para janela de filtro de gravação:** Verificar essa opção se você quiser forçar o dispositivo para desautorizar a escritura em uma hora exata (re-habilitando o filtro de escritura, enhanced ou baseado em arquivo, e reiniciando imediatamente na Hora de término selecionada).
- **Hora final:** Especifica uma hora exata quando a escritura no dispositivo termina, de acordo com o método descrito acima.

AVISO: Novamente: a especificação de uma hora de término para a janela de filtro de gravação fará com que a máquina reinicie imediatamente quando atingir esta hora e o dispositivo retornará ao estado de filtro de gravação habilitado

Distribuição da Descoberta estendida de dispositivos

A Descoberta estendida de dispositivos é uma extensão da ferramenta de descoberta de dispositivos não gerenciados . Localiza dispositivos na sua rede, os quais não enviaram uma análise de inventário ao banco de dados núcleo. Com a descoberta estendida de dispositivos, você pode usar um ou ambos dos seguintes métodos de descoberta: Descoberta ARP (address resolution protocol - protocolo de resolução de endereço) e descoberta WAP (wireless access point - ponto de acesso sem fio).

Sobre a página Descoberta estendida de dispositivos

Use esta página para habilitar e configurar a descoberta estendida de dispositivos nos dispositivos gerenciados com esta configuração de agente.

Com a descoberta ARP, o agente de descoberta estendida de dispositivos procura por transmissões ARP de rede. Em seguida o agente verifica quaisquer dispositivos descobertos por ARP para verificar se possuem o agente LANDesk padrão instalado. Se o agente LANDesk não responder, o dispositivo descoberto por ARP é exibido na lista Computadores. A descoberta estendida de dispositivo é ideal nas situações que envolvem firewalls as quais impedem os dispositivos de responderem aos métodos de descoberta UDD baseada em ping.

Lembre-se que não é necessário distribuir o agente de descoberta estendida de dispositivos em todos os dispositivos gerenciados da sua rede, embora você possa, caso deseje. A distribuição deste agente para vários dispositivos em cada sub-rede deve dar a cobertura suficiente.

Essa página contém as seguintes opções:

- **Use ARP (Address Resolution Protocol):** Habilita a descoberta estendida de dispositivos usando o método de descoberta de protocolo de resolução de endereço (ARP) nos dispositivos com essa configuração de agente.
- **Escolher uma configuração de descoberta ARP:** Especifica a configuração de ARP que controla o agente de descoberta estendida de dispositivo ao executar a descoberta ARP em sua rede. As configurações de ARP determinam a freqüência de análise de descoberta e o nível de registro. Selecione uma configuração da lista disponível para aplicá-la à configuração do agente que está sendo criado. Se desejar, clique em **Configure** para criar e aplicar uma nova configuração de análise e reparo ou para editar uma já existente.
- **Use WAP (Wireless Access Point discovery):** Habilita a descoberta estendida de dispositivos usando o método de descoberta de protocolo de resolução de endereço (ARP) nos dispositivos com essa configuração de agente.
- **Escolher uma configuração de descoberta WAP:** Especifica a configuração de ARP que controla o agente de descoberta estendida de dispositivo ao executar a descoberta ARP em sua rede. As configurações de WAP determinam a freqüência de análise de descoberta e o nível de registro. Selecione uma configuração a partir da lista **Suspensa** para aplicá-la à configuração que está sendo criada Se desejar, clique em **Configurar** para criar e aplicar uma nova configuração ou para editar uma já existente.
- **Freqüência de download da configuração (em minutos):** Especifica a freqüência com que os dispositivos gerenciados com agente de descoberta estendida de dispositivo contatam o servidor núcleo para uma configuração atualizada de descoberta estendida de dispositivo. O agente sempre atualiza sua configuração do núcleo quando ele é carregado inicialmente. O valor padrão é de 720 segundos (12 minutos). Se você definir esse valor muito alto, as configurações levarão muito tempo para se propagarem para os dispositivos. Se você definir esse valor muito baixo, aumentará a carga no servidor núcleo e na rede.

Distribuição do gerenciamento de energia

A funcionalidade LANDesk Power Management permite aos administradores controlar centralmente o consumo de energia de nó final facilitando a criação, avaliação financeira e distribuição de diretivas de gerenciamento de energia.

Sobre a página de Gerenciamento de energia

Use a página de Gerenciamento de energia para selecionar a diretiva de energia a ser distribuída para o computador cliente. Embora os administradores controlem centralmente as condições sob as quais os computadores e monitores ficam em tempo de espera, hibernam ou são desativados, os usuários podem impedir ações específicas de Gerenciamento de energia no cliente, se necessário. Além disso, uma opção de desligamento “suave” protege os dados não salvos do usuário. Um banco de dados pré-povoado de valores de consumo de wattagem do OEM é correspondido com os dados de inventário de hardware e as configurações de wattagem personalizada disponíveis permitem altos níveis de precisão na estimativa de economia financeira e de energia.

A janela do Gerenciamento de energia página contém os seguinte recursos:

- **O uso da diretiva de energia no cliente:** Habilita o gerenciamento de energia nesta configuração de agente.
- **Configurações da diretiva de energia:** Selecione uma diretiva de energia que foi criada e configurada para ser usado em dispositivos gerenciados.
- **Escolher uma diretiva de energia:** Especifica a diretiva de energia que será enviada com a configuração de agente. Como padrão, existirá uma ou nenhuma diretiva de energia disponível
- **Coletar info de uso do cliente:** Coleta o uso da energia da utilização individual de cliente. Essas informações são usadas para criar relatórios mais precisos de uso de energia para saber as demandas exatas de energia dos dispositivos e monitores que estão conectados a eles.
- **Configurar:** Permitem criar, editar, copiar e excluir perfis de gerenciamento de energia.

Distribuição do Desktop Manager

O Desktop Manager melhora a experiência do usuário final ao oferecer uma UI consolidado do cliente de desktop que inclui acesso a ambos, ao Portal de Distribuição de software e ao console LaunchPad, a partir de um único atalho do menu Iniciar.

Sobre a página Desktop Manager

Usar as páginas do Gerenciador de desktop para configurar como o Gerenciador de desktop aparecerá.

Essa página contém as seguintes opções:

- **Aplicativos disponíveis:** Contém os aplicativos que podem ser configurados para acesso através do Desktop Manager. Os aplicativos disponíveis são:
  - **LaunchPad:** Um console que fornece acesso a pacotes, executáveis, URLs e links de gerenciamento de processo que foram configurados individualmente para um dispositivo. O LaunchPad fornece acesso em um clique para aplicativos locais, hospedados ou "just-in-time" que não são instalados até que um usuário final clique no ícone.
  - **Portal de distribuição de software:** Mostra todos os pacotes de distribuição que foram distribuídos com o uso de um método de entrega baseado em diretiva opcional ou recomendado.
- **Exibir no Desktop Manager:** Exibe os aplicativos que serão exibidos e acessados através do Desktop Manager. Use a opção >> e << para selecionar ou desselecionar os aplicativos desejados. Como padrão ambos, o LaunchPad e o Portal de distribuição de software estão inclusos.

Sobre a página Personalização (no Desktop Manager)

Usar a página de Personalização para configurar local de atalhos selecionados para o Gerenciador de desktop e iniciar ou desligar preferências.

A página de Personalização contém as seguintes características:

- **Grupo de programas LANDesk:** Cria um menu Iniciar no grupo de programas LANDesk.
- **Desktop do Windows:** Cria um atalho na desktop.
- **Menu Iniciar do Windows:** Cria uma entrada do menu Iniciar.
- **Executar o Desktop Manager quando o usuário fizer o login:** Executa o Desktop Manager automaticamente quando o usuário faz o login no dispositivo gerenciado.
- **Não permitir que o Desktop Manager seja fechado:** Impede que os usuários finais fechem a janela do Desktop Manager.

Sobre a página Marcas (em Desktop Manager)

Usar a página Branding para personalizar o conteúdo e aparência do Gerenciador de desktop.

A página de Branding contém as seguintes características:

- **Título do aplicativo:** Permite a personalização do titulo da janela do aplicativo. O padrão é LANDesk Desktop Manager.
- **A sua mensagem:** Permite a um administrador digitar uma mensagem personalizada para ser mostrada na área central inferior do Desktop Manager. Como padrão nenhuma mensagem é exibida.
- **Ícone corporativo:** Adiciona um arquivo de ícone que substitui o ícone padrão no Desktop Manager. O ícone selecionado no canto esquerdo superior próximo do “Portal de distribuição de software”.
- **Logotipo corporativo:** Adiciona um logotipo da empresa que aparece no canto esquerdo inferior da janela. O logotipo LANDesk sempre aparece no canto direito inferior.

Uso do Utilitário de configuração do cliente

Sobre a caixa de diálogo Utilitário de configuração do cliente

A caixa de diálogo de utilidade da configuração de agente exibe o status de uma tarefa de configuração de um dispositivo agendado enquanto a tarefa é processada. Esta caixa de diálogo é apenas informativo; os dispositivos a serem configurados foram selecionados quando a tarefa foi agendada.

A caixa de diálogo do utilitário de Configuração de agente contém os seguintes recursos:

- **Clientes a serem configurados:** Contém os dispositivos agendados para receber essas configurações.
- **Clientes sendo configurados:** Lista os dispositivos que foram contatados pelo console e que estão sendo configurados com esse arquivo de configurações.
- **Clientes concluídos:** Contém os dispositivos que o console configurou durante essa sessão agendada. Se a tentativa de configuração for bem-sucedida, o status será Concluído. Se a tentativa de configuração falhar por qualquer motivo, o status será Falhou. Esses status são espelhados na janela Tarefas agendadas quando essa tarefa é selecionada.
- **Criação de arquivos de configuração:** Mostra uma barra de status indicando o status de conclusão da tarefa de configuração inteira.

Sobre a caixa de diálogo Adicionar um servidor bare metal.

Use a caixa de diálogo Adicionar um servidor bare metal para adicionar dispositivos à fila, o que fará com que as tarefas de provisionamento sejam executadas nos mesmos. Essa ação é particularmente útil para a provisão inicial de novos dispositivos. Os dispositivos são adicionados à fila de retenção usando-se um identificador. Um identificador de servidor pode ser usado para identificar de forma exclusiva um servidor. Um identificador de servidor pode ser um endereço MAC (mais comum), o número de série de um fornecedor, um GUID IPMI ou um GUID Intel vPro. Em todos os casos, o identificador deve ser pesquisado por um agente rodando no ambiente de pré-inicialização no servidor alvo.

Você pode acrescentar dispositivos individualmente ou vários ao mesmo tempo. Se você adiciona muitos dispositivos, você precisa criar um arquivo de texto no formato CSV com dados dos dispositivos. Você importará este arquivo para adicionar dispositivos à fila.

Para adicionar um único dispositivo

1. Na **Tela de rede**, expanda o grupo **Configuração**. Com o botão direito clique em **Servidor bare metal** e depois em **Adicionar dispositivos**.
2. Clique em **Adicionar**. Digite um nome descritivo na caixa de texto **Nome**. Apesar de o nome de exibição ser opcional, ele é enfaticamente recomendado. Em dispositivos bare metal, o nome de exibição é o único diferenciador na tela de Provisionamento.
3. Selecione um tipo na lista **Tipo de identificador** (endereço Mac, número de série, GUID IPMI ou GUID Intel vPro) e insira o valor na caixa de texto **Identificador**. Clique em **Adicionar**.
4. Repete as etapas de 2 a 3 para adicionar outros dispositivos. Você pode também adicionar outros identificadores para o dispositivo; é só adicionar outro identificador com o mesmo nome de exibição.
5. Clique em **OK**.

Para adicionar vários dispositivos

1. Na **Tela de rede**, expanda o grupo **Configuração**. Com o botão direito clique em **Servidor bare metal** e depois em **Adicionar dispositivos**.
2. Na lista **Tipo de identficador**, selecione um tipo de identificador que corresponda aos dados que você irá importar.
3. Digite o local do arquivo de texto (CSV) que contém as informações do identificar na caixa de texto (ou clique em **Procurar** para encontrar o arquivo) e clique em **Importar**.

Cada identificador deve estar separado por vírgula no arquivo CSV. A importação do formato de arquivo é nome de tela, identificador.

Distribuição de Configuração de agente para Servidores Linux e UNIX

Você pode usar a ferramenta de configuração do agente do console para distribuir agentes para os sistemas operacionais Linux e UNIX suportados. Para obter mais informações sobre a distribuição do agente Linux, consulte "Configuração de agentes de dispositivos Linux e UNIX" na página 112.

Sobre a página Iniciar (em Configuração do Agente Linux/UNIX)

A página Iniciar da Configuração de agentes Linux contém as seguintes opções:

- **Nome de configuração:** Digite um nome que descreva a configuração em que você está trabalhando. O nome pode ser o nome de uma configuração existente ou um novo nome. Esse nome é exibido na janela **Configuração de agentes**.

- **Agente padrão da LANDesk**, **Controle remoto** e **Distribuição de software**: Essas opções são instaladas como padrão e podem ser desativadas.
- **Analisador de vulnerabilidades do LANDesk:** Instala a versão Linux do Analisador de vulnerabilidades. O analisador só reporta os problemas, ele não os corrige.
- **Inventário e monitoramento em tempo real:** Instala um agente que oferece suporte ao inventário e monitoramento em tempo real do console do LANDesk Management Console.
- **Padrões:** Redefine as opções para padrão (desativa a opção **Analisador de vulnerabilidades** do **LANDesk)**.

Sobre a página Agente LANDesk padrão (sob a configuração de agente Linux/UNIX)

A página da Configuração de agente Agente LANDesk padrão LINUX tem essas opções:

- **Certificados confiáveis para autenticação do agente:** os certificados controlam quais servidores núcleo podem gerenciar dispositivos. Selecione os certificados do servidor núcleo que deseja instalar com esta configuração. Para obter mais informações, consulte "Segurança de agente e certificados confiáveis" na página 108.
- **NOTA:** As outras opções nesta página estão esmaecidas e não se aplicam às configurações de agente Linux.

Sobre a página Analisador de inventário (em Configuração do Agente Linux/UNIX)

A página do Analisador de inventário da Configuração de agentes Linux contém as seguintes opções:

- **Iniciar análise de inventário:** Selecione **Diário, Semanal ou Mensal**. A opção que selecionar adiciona um comando ao arquivo cron.daily, cron.weekly ou cron.monthly do servidor que executa o analisador de inventário.

Monitorador de agentes (Agente Watcher)

Visão geral do Agent Watcher

O Agent Watcher LANDesk permite monitorar de forma ativa o status dos serviços de agente e de arquivos selecionados do LANDesk Management Suite a fim de garantir sua integridade e preservar o funcionamento correto em dispositivos gerenciados. O Agent Watcher pode ser habilitado e as configurações a ele associadas podem ser distribuídas com uma configuração inicial de agente de dispositivo. Ele também pode ser atualizado a qualquer momento sem a necessidade de uma configuração completa de agente.

O Agent Watcher não somente monitora os serviços e arquivos críticos, como também reinicia serviços terminados, reinicia serviços configurados para início automático, restaura arquivos com eliminação pendentes na reinicialização e informa o servidor núcleo sobre evidências de manipulação indevida do arquivo.

O Agent Watcher monitora os serviços e arquivos do agente LANDesk Management Suite especificados pelas configurações de um Agent Watcher de um dispositivo.

As configurações do Agent Watcher também determinam a freqüência de verificação de status de serviços e arquivos do agente, determinam se o Agent Watcher fica residente nos dispositivos e se devem ser verificadas mudanças nas próprias configurações.

Como padrão, o Agent Watcher está desativado. Você pode ativá-lo com uma configuração de agente ou posteriormente, através de uma tarefa separada de atualização das definições do Agent Watcher. Em outras palavras, você pode ter que ativar o Agent Watcher durante a configuração inicial do dispositivo. Isso pode ser feito a qualquer momento do console para um ou mais dispositivos gerenciados.

Ao monitorar serviços e arquivos, o agent watcher executa as ações recuperativas descritas abaixo.

Plataformas de dispositivo suportadas e requisitos de sistema

O Agent Watcher suporta a maioria das mesmas plataformas suportadas pelo Management Suite, inclusive os seguintes sistemas operacionais (relacionados abaixo com os requisitos mínimos de software e hardware):

- **Microsoft Windows XP 64 bit Professional**
  (Processador Intel Pentium 64 bits ou compatível; 128 MB de RAM, sendo recomendado mais; 72 MB disponível no disco rígido para instalação)
- **Windows 2000 Professional**
  (SP2 ou mais recente; processador Intel Pentium de 133 MHz ; 96 MB de RAM, são recomendados 96 MB; 50 MB disponível no disco rígido para instalação)
- **Microsoft Windows XP Professional**
  (Microsoft Internet Service Pack 2.0 ou mais recente; processador Intel Pentium de 300 MHz ou compatível; 128 MB de RAM, é recomendado mais; 72 MB disponível no disco rígido para instalação)

Monitore serviços e arquivos com Agent Watcher

Você pode usar o LANDesk Agent Watcher para monitorar os serviços e arquivos a seguir.

Monitoramento de serviços

Os seguintes serviços de agente podem ser monitorados:

- Agendador local
- Antivírus
- Controle remoto
- Monitoramento de software
- Multidifusão dirigida

CUIDADO: Os serviços que não estiverem sendo distribuídos não devem ser selecionados para monitoramento pelo Agent Watcher
Ao definir as configurações do agent watcher, não selecione serviços que não pretende instalar nos dispositivos alvo. Se o fizer, o servidor núcleo receberá alertas para serviços que não estão sendo instalados e que não foram instalados de propósito. Entretanto, observe que mesmo se um serviço que não foi instalado for selecionado para monitoramento, não serão enviados alertas informando que o serviço não pode ser reiniciado ou que seu tipo de início não pode ser mudado.

Ao monitorar serviços de agente, o Agent Watcher:

- Reinicia serviços quando estão desligados (uma vez).
- Muda o tipo de reinicialização de serviço de volta para automático quando o tipo é mudado
- Envia alertas ao servidor núcleo quando serviços não estão instalados.
- Envia alertas ao servidor núcleo quando os serviços não podem ser reiniciados.
- Envia alertas ao servidor núcleo quando um tipo de reinicialização de serviço não pode ser mudado de volta para automático.

Monitoramento de arquivos

Os seguintes arquivos podem ser monitorados:

- Ldiscn32.exe
- Vulscan.dll
- Vulscan.exe
- Sdclient.exe

Ao monitorar arquivos, o Agent Watcher:

- Remove do registro os arquivos que foram agendados para exclusão na reinicialização
- Envia alertas ao servidor núcleo quando os arquivos são agendados para exclusão na reinicialização.
- Envia alertas ao servidor núcleo quando os arquivos forem excluídos.

Habilitar e configurar o Agent Watcher

O utilitário LANDesk Agent Watcher é instalado com o agente Management Suite standard, mas como padrão, está desativado.

O Agent Watcher pode ser ativado através da configuração inicial do agente do dispositivo ou posteriormente através de uma tarefa de atualização das configurações do Agent Watcher.

Habilite o Agent Watcher em dispositivos

Para habilitar o Agent Watcher durante a configuração do agente

1. No console, clique em **Ferramentas > Configuração > Configuração de agentes**.
2. Clique no botão da barra de ferramentas **Nova configuração de agente do Windows**.
3. Após especificar os parâmetros desejados para a configuração do agente, clique no grupo **Segurança e conformidade** e, a seguir, clique no **Agent Watcher** para abrir a página na caixa de diálogo.
4. Marque **Usar Agent Watcher**.
5. Selecione uma das configurações da lista disponível para aplicá-la à configuração do agente que está criando. Você também pode criar novas configurações ou editar configurações existentes. A configuração aplicada determina que serviços e arquivos são monitorados e com que freqüência, e se o executável do Agent Watcher permanecerá residente na memória dos dispositivos monitorados.
6. Termine de especificar as definições para a configuração do agente e clique em **Salvar**.

Se quiser ativar o Agent Watcher (ou atualizar as configurações do mesmo) posteriormente, isso pode ser feito em um ou mais dispositivos diretamente do console.

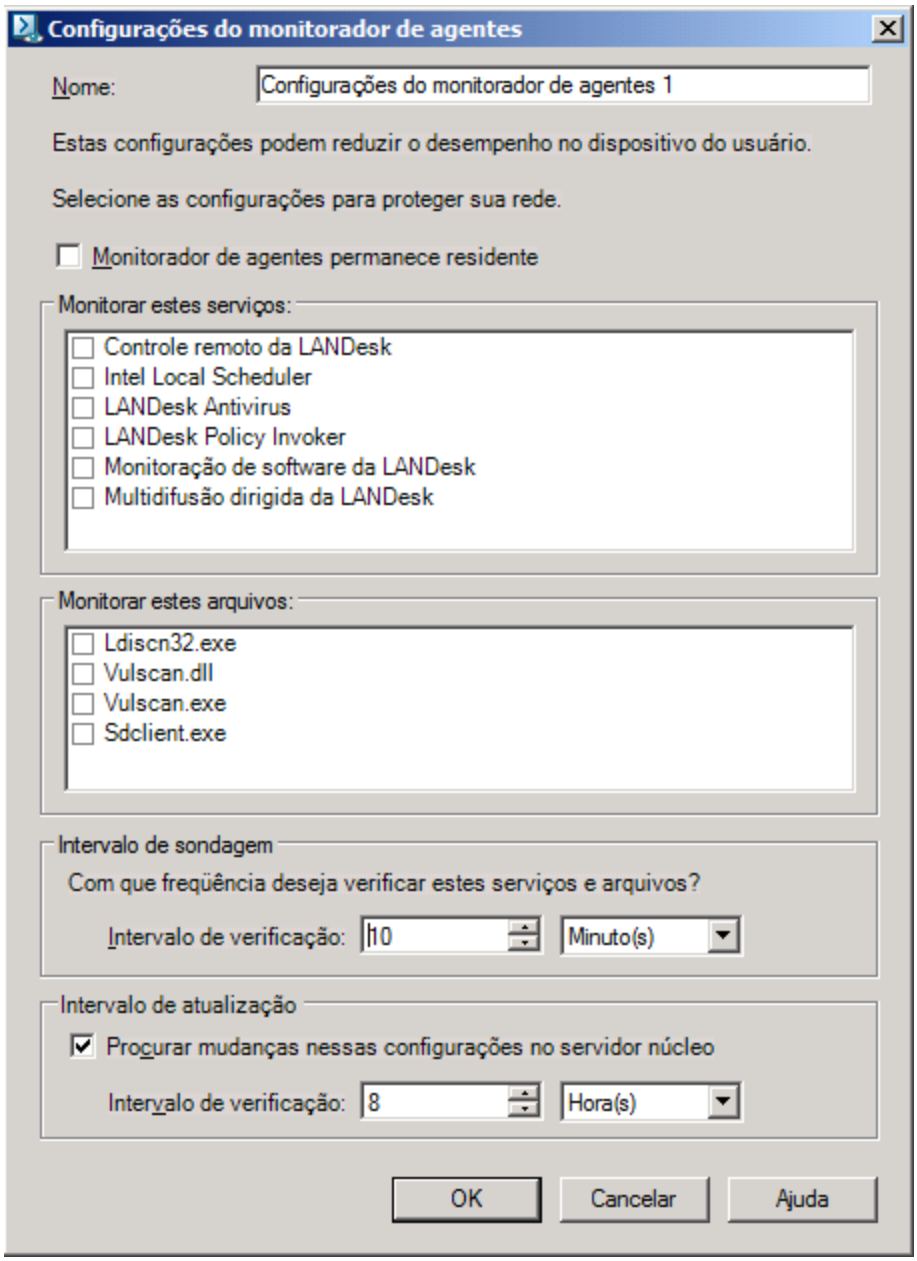
Para habilitar o Agent Watcher (ou atualizar as configurações) como uma tarefa separada

1. No console, clique com o botão direito em um ou mais dispositivos e, em seguida clique em **Atualizar as configurações do Agent Watcher**.
2. Marque **Usar Agent Watcher**.
3. Selecione uma das configurações da lista disponível para aplicá-la à configuração do agente que está criando. Você também pode criar novas configurações ou editar configurações existentes. A configuração aplicada determina que serviços e arquivos são monitorados e com que freqüência, e se o executável do Agent Watcher permanecerá residente na memória dos dispositivos monitorados.
4. Clique em **OK**.

Ao clicar no botão **OK**, todos os dispositivos selecionados são atualizados com as novas configurações e aparece uma mensagem de status.

Configurar parâmetros do Agent Watcher

Use as configurações do Agent Watcher (clique em **Ferramentas > Configuração > Configuração de gente > Nova configuração de agente do Windows > Segurança e conformidade > Agent Watcher**) para determinar os serviços e arquivos a serem monitorados, a frequência de verificação de status de serviços e arquivos, se o Agent Watcher fica residente nos dispositivos e se devem ser verificadas mudanças nas configurações aplicadas.



Desabilitar o Agent Watcher em dispositivos

É possível também desativar o Agent Watcher de um ou mais dispositivos com a tarefa de atualização do Agent Watcher.

Para desabilitar o Agent Watcher

1. No console, clique com o botão direito em um ou mais dispositivos e, em seguida clique em **Atualizar as configurações do Agent Watcher**.
2. Certifique-se que a caixa de seleção **Usar Agent Watcher** está desmarcada.
3. Clique em **OK**.

Gerar relatórios do Agent Watcher

Informações de monitoramento e alertas do Agent Watcher são apresentadas na ferramenta Relatórios.

Todos os relatórios do Agent Watcher incluem o nome de host da estação de trabalho, o serviço ou arquivo monitorado, o status do alerta (encontrado ou resolvido) e a data em que o evento foi descoberto.

O Agent Watcher grava o estado dos alertas para que o núcleo receba somente um alerta quando a condição é encontrada e um alerta quando a condição é resolvida. Podem ocorrer vários alertas quando o Agent Watcher é reiniciado para reinicializar o sistema ou quando houver uma nova definição por envio ou recepção na estação de trabalho.

Relatórios também podem ser gerados para uma dada categoria com base em intervalos de tempo diferentes, como hoje, semana passada, últimos 30 dias ou outro intervalo especificado.

IMPORTANTE: Os **dados de alerta do Agent Watcher são removidos automaticamente após 90 dias**
Todos os alertas do Agent Watcher que tiverem mais que 90 dias serão removidos automaticamente do banco de dados. Os dados de alerta são usados para gerar relatórios do Agent Watcher.

IMPORTANTE: P**ermissões e funções necessárias para usar a ferramenta Relatórios**
Para acessar a ferramenta Relatórios, gerar e exibir relatórios, o usuário precisa ter direitos de administrador LANDesk (o que implica direitos plenos) ou direitos específicos para a função de Relatórios.

Para obter mais informações sobre o uso da ferramenta Relatórios, consulte "Relatórios" na página 197.

Relatórios do Agent Watcher

Os relatórios do Agent Watcher estão relacionados abaixo:

Falha na mudança do tipo de serviço

Esse relatório contém todos os alertas do Agent Watcher nas estações de trabalho incapazes de mudar o tipo de inicialização de um serviço monitorado.

Serviços requeridos não instalados

Esse relatório contém todos os alertas do Agent Watcher nas estações de trabalho onde um serviço monitorado foi desinstalado.

Serviços requeridos não iniciados

Esse relatório contém todos os alertas do Agent Watcher nas estações de trabalho onde um serviço monitorado não pode ser reiniciado pelo Agent Watcher.

Arquivos não encontrados nos clientes

Esse relatório contém todos os alertas do Agent Watcher nas estações de trabalho onde os arquivos de agente monitorados foram excluídos.

Arquivos pendentes excluídos encontrados no cliente

Esse relatório contém todos os alertas do Agent Watcher nas estações de trabalho onde os arquivos de agente monitorados foram agendados para exclusão na reinicialização. O Agent Watcher também remove automaticamente esses arquivos do registro do Windows para que não sejam excluídos.

Ajuda do Agent Watcher

Essa seção contém os seguintes tópicos de ajuda que descreve as mensagens do Agent Watcher.

Sobre a caixa de diálogo Configuração das definições do Agent Watcher

Use caixa de diálogo para gerenciar suas configurações. Uma vez configurado, as configurações a dispositivos gerenciados através de uma configuração de agente ou de uma tarefa de modificação de configurações.

O Agent Watcher permite criar configurações variadas que podem ser aplicadas a dispositivos ou a grupos de dispositivos.

Esta caixa de diálogo contém as seguintes opções:

- **Novo:** Abre a caixa de diálogo de configurações onde você pode configurar as opções.
- **Editar:** Abre a caixa de diálogo de definições onde você pode modificar as configurações selecionadas.
- **Copiar:** Abre uma cópia das configurações selecionadas como um modelo que pode ser modificado e renomeado.
- **Excluir:** remove as configurações selecionadas do banco de dados.
- **Fechar:** Fecha a caixa de diálogo sem aplicar nenhuma configuração à tarefa.

Sobre a caixa de diálogo Configurações do Agent Watcher

Use esta caixa de diálogo para criar e editar ad configurações do Agent Watcher.

As definições do Agent Watcher determinam quais serviços e arquivos são monitorados e a respectiva freqüência, e se o utilitário permanece residente no dispositivo.

Esta caixa de diálogo contém as seguintes opções:

- **Nome:** Identifica as configurações com um nome exclusivo.
- **O Agent Watcher permanece residente:** Indica se o LDRegwatch.exe (executável do Agent Watcher) permanece o tempo todo residente na memória. Se você não marcar essa opção, o LDRegwatch.exe só permanecerá memória o tempo suficiente para verificar os serviços e arquivos selecionados na hora agendada.
- **Monitorar esses serviços:** Especifica quais serviços críticos serão monitorados com essas configurações do Agent Watcher.
- **Monitorar esses arquivos:** Especifica quais arquivos críticos serão monitorados com essa configuração do Agent Watcher.
- **Intervalo de sondagem:** Especifica a freqüência desejada para que o Agent Watcher monitore os serviços e arquivos selecionados. O valor mínimo para esse intervalo é de 30 segundos.

- **Procure mudanças a essas configurações no servidor núcleo:** Compara automaticamente a versão das definições do Agent watcher selecionado com a que foi distribuída aos dispositivos alvo (no intervalo abaixo especificado). Se as configurações foram modificadas durante o intervalo, as novas configurações do Agent Watcher são distribuídas e ele é reiniciado com as novas configurações.
    - **Intervalo de verificação:** especifica o período da comparação recorrente das configurações do Agente Watcher.

IMPORTANTE: Os serviços que não estiverem sendo distribuídos não devem ser selecionados para monitoramento pelo Agent Watcher
Ao definir as configurações do agent watcher, não selecione serviços que não pretende instalar nos dispositivos alvo. Se o fizer, o servidor núcleo receberá alertas para serviços que não estão sendo instalados e que não foram instalados de propósito. Entretanto, observe que mesmo se um serviço que não foi instalado for selecionado para monitoramento, não serão enviados alertas informando que o serviço não pode ser reiniciado ou que seu tipo de início não pode ser mudado.

Sobre a caixa de diálogo Atualização das configurações do Agent Watcher

Use esta caixa de diálogo para atualizar as configurações do Agent Watcher nos dispositivos alvo e para habilitar ou desabilitar o utilitário Agente Watcher nos dispositivos alvo.

Se o Agent Watcher não estiver ativo nas estações de trabalho selecionadas, marque a caixa de seleção **Uso do Agent Watcher**, configure as definições do mesmo e, em seguida, **OK**. O Agent Watcher será ativado depois que a configuração tiver sido enviada aos dispositivos selecionados. Para mudar os arquivos ou serviços que são monitorados, clique no botão **Configurar** para mostrar a caixa de diálogo **Configurações do Agent Watcher**.

Na caixa de diálogo Atualização das configurações Agent Watcher você também pode desativá-lo, desmarcando a caixa de seleção **Uso do Agent Watcher** e clicando em **OK**.

Esta caixa de diálogo contém as seguintes opções:

- **Usar Agent watcher:** Habilita o serviço do Agent watcher nos dispositivos alvo.
- **Escolher uma configuração do Agent Watcher:** Especifica quais configurações são usadas para a tarefa. Selecione uma das configurações da lista ou clique em **Configurar** para criar novas configurações.

Quando o botão **OK** é selecionado, todos os dispositivos selecionados são atualizados com as novas configurações e aparece uma mensagem de status.

Inventário

Visão geral da análise de inventário

A análise de inventário coleta os dados de hardware e software e os insere no banco de dados núcleo. Ao configurar um dispositivo com a Ferramenta de configuração de agente, a varredura (analisador) de inventário é um dos componentes do agente Management Suite padrão instalados no dispositivo. A análise de inventário é automaticamente executada quando o dispositivo é inicialmente configurado. Um dispositivo é considerado gerenciado quando envia uma análise de inventário ao banco de dados núcleo. O executável da varredura é denominado ldiscn32.exe.

Há dois tipos de análise de inventário:

- **Análise de hardware**: Análises de dados de hardware em dispositivos gerenciados A análise de hardware é executada rapidamente. É possível configurar o intervalo de análise de hardware em uma configuração de agente (**Ferramentas > Configuração > Configuração de agente**), que pode ser distribuído para dispositivos gerenciados. Como padrão, as análises de hardware são executadas toda vez que o dispositivo inicializa.
- **Análise de software**: Análises de software instalados em dispositivos gerenciados. Essas análises levam mais tempo para serem executadas que as análises de hardware. As análises de software podem levar alguns minutos para terminar, dependendo do número de arquivos no dispositivo gerenciado. Como padrão, a análise de software é executada uma vez por dia, indiferente da frequência de execução da varredura de inventário no dispositivo. O intervalo de análise de software pode ser configurado na guia **Configurar > Serviços > Inventário**.

Você pode analisar um dispositivo por demanda, procurando-o na tela de rede, clique nele com o botão direito e depois em **Análise de inventário**.

NOTA: Um dispositivo adicionado ao banco de dados núcleo, usando o recurso descoberta ainda não terá analisado seus dados de inventário no banco de dados núcleo. É preciso executar uma varredura de inventário em cada dispositivo para que todos os dados de inventário sejam exibidos para esse dispositivo.

Você pode ver os dados de inventário e usá-los para:

- Personalizar as colunas da tela de rede para exibir os atributos de inventário específicos
- Consultar o banco de dados núcleo quanto a dispositivos com atributos de inventário específicos
- Agrupar dispositivos para designar tarefas de gerenciamento, como distribuição de software
- Gerar relatórios especializados com base nos atributos de inventário

Também é possível usar as varreduras de inventário para manter o controle das alterações de hardware e software nos dispositivos e gerar alertas ou entradas no arquivo de log quando tais alterações ocorrem. Para obter mais informações, consulte "Controle das mudanças no inventário" na página 151.

Otimização análise de inventário

As informações a seguir descrevem algumas das opções disponíveis para otimização das análises de inventário.

Análise delta

Depois que a análise completa inicial é executada em um dispositivo, a análise de inventário captura apenas as modificação delta e as envia ao banco de dados núcleo. Ao enviar somente os dados modificados, o tráfego da rede e o tempo de processamento de dados são minimizados.

Como forçar uma análise completa

Se quiser forçar uma análise completa dos dados de hardware e software do dispositivo, você pode excluir o arquivo delta de análise atual e mudar um parâmetro no miniaplicativo Configurar serviços do Software LANDesk (**Configurar > Serviços**).

1. Apague o arquivo **invdelta.dat** do dispositivo. Há uma cópia da última análise de inventário armazenada localmente como arquivo oculto denominado invdelta.dat A variável de ambiente LDMS_LOCAL_DIR define o local desse arquivo. Como padrão o local é C:\Arquivos de programa\LANDesk\LDClient\Data.
2. Adicione a opção **/sync** à linha de comandos do utilitário de análise de inventário. Para editar a linha de comandos, clique em **Iniciar > Todos os programas > Gerenciamento LANDesk**, clique com o botão direito no ícone de atalho **Análise de inventário**, selecione **Propriedades > Atalho** e edite o caminho **Alvo**.
3. No servidor núcleo, clique em **Iniciar > Todos os programas > LANDesk > Configurar serviços LANDesk**.
4. Clique na guia **Inventário** e clique em **Configurações avançadas**.
5. Clique no parâmetro **Do Delta** (Executar Delta). Digite **0** na caixa **Valor**.
6. Clique em **OK** duas vezes e clique em **Sim** ao ser avisado para reiniciar o serviço.

Compactação da análise

As análises de inventário executadas pela análise de inventário do Windows (ldiscn32.exe) são compactadas por padrão. A análise compacta as análises completas e delta com uma taxa de compactação de aproximadamente 8:1. Em primeiro lugar, as análises são compiladas totalmente na memória, em seguida, são compactadas e enviadas ao servidor núcleo usando um tamanho de pacote maior. A compactação da análise requer menos pacotes e reduz o uso da largura de banda.

Criptografia da análise

Por padrão, as análises de inventário são criptografadas (apenas análises de TCP/IP). Você pode desativar a criptografia da análise de inventário mudando um parâmetro no miniaplicativo Configurar serviços **(Configurar > Serviços)**.

1. No servidor núcleo, clique em **Iniciar > Todos os programas > LANDesk > Configurar serviços**LANDesk.
2. Clique na guia **Inventário** e clique em **Configurações avançadas**.
3. Clique no parâmetro **Disable Encryption**. Digite **1** na caixa **Valor**.
4. Clique em **Definir**, em seguida clique em **OK**.
5. Clique em **OK,** e depois em **Sim** ao ser avisado para reiniciar o serviço.

Dados criptografados de transporte

Em **Configurar > Serviços >** guia **Inventário** há uma opção **Dados criptografados de transporte**. Essa opção faz as análises do dispositivo serem enviadas ao núcleo com uso de SSL. Os arquivos são enviados através do Serviço de web e não do front end do serviço de inventário, portanto, não será anexado o endereço NAT ao arquivo de análise, mesmo se essa opção estiver ativada no registro.

Visualização dos dados de inventário

Quando um dispositivo é analisado pela análise de inventário, é possível ver suas informações de sistema no console.

Os dados de inventários do dispositivo são armazenados no banco de dados núcleo e incluem as informações de hardware, driver de dispositivo, software, memória e ambiente. É possível usar o inventário para ajudar a gerenciar e configurar dispositivos e a identificar problemas no sistema rapidamente.

Você pode ver os dados do inventário como um resumo ou como um inventário completo do dispositivo. Também é possível ver os dados de inventário em relatórios que você gera. Para obter mais informações, consulte "Relatórios" na página 197.

Como ver o resumo de inventário

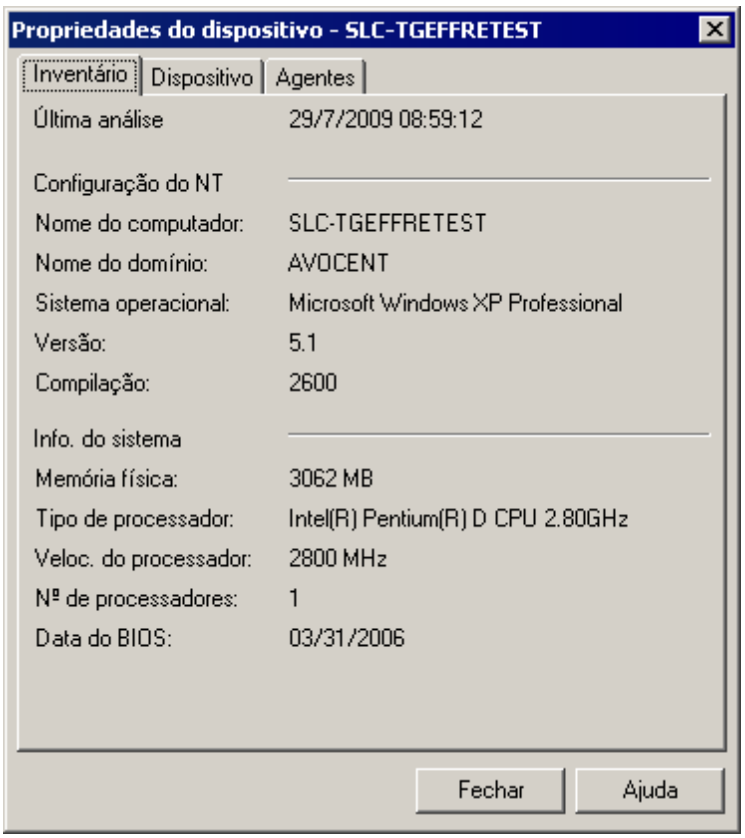
O inventário de resumo é encontrado na página de propriedades do dispositivo e fornece uma breve análise das informações do sistema e da configuração básica do SO do dispositivo. O resumo também mostra a data e a hora da última análise de inventário para que você saiba se os dados são atuais.

NOTA: Se você adicionou um dispositivo ao banco de dados núcleo usando a ferramenta de descoberta, seus dados de inventário ainda não terão sido analisados no banco de dados núcleo. Você deve executar uma análise de inventário no dispositivo antes que você possa vê-lo.

Para ver o resumo de inventário

1. Na tela de rede do console, clique com o botão direito do mouse em um dispositivo.
2. Clique na guia **Propriedades** > **Inventário**.

Exibir/ocultar imagens



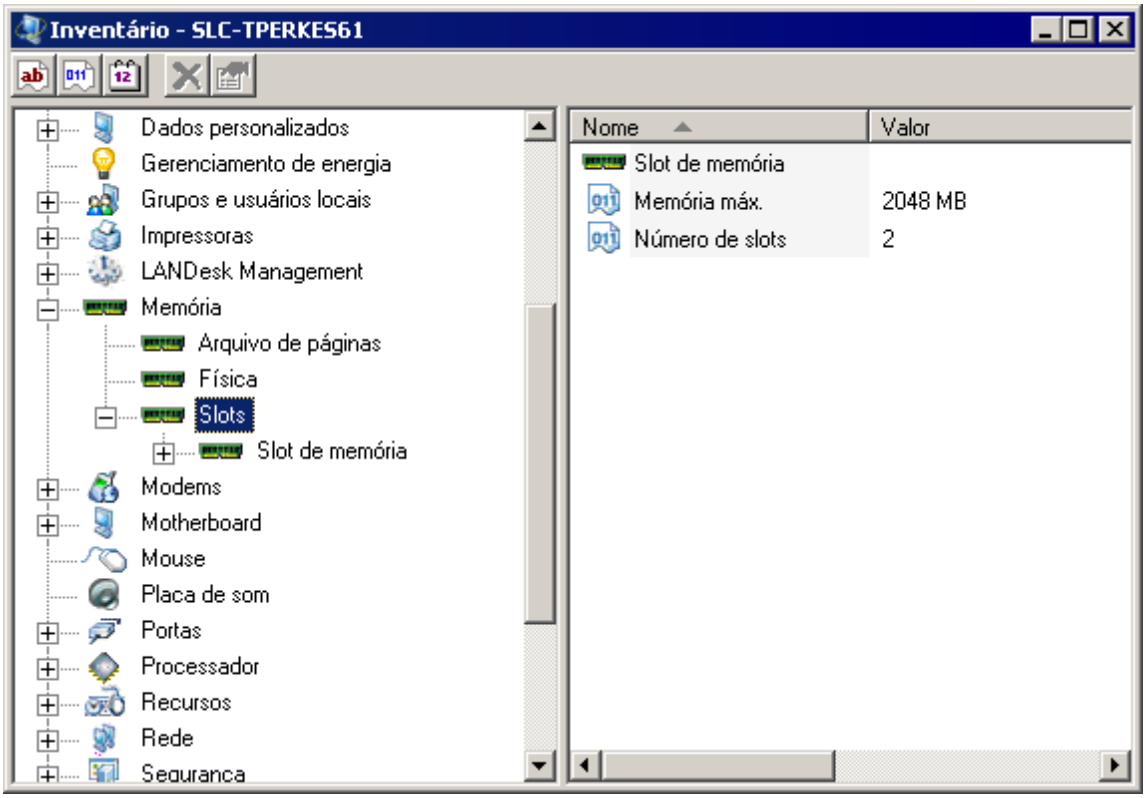
Visualização de um inventário completo

Um inventário completo fornece uma listagem completa dos componentes de hardware e software detalhados de um dispositivo. A lista contém objetos e atributos de objetos.

Para ver um inventário completo

1. Na tela de rede do console, clique com o botão direito do mouse em um **dispositivo**.
2. Clique em **Inventário**.

Exibir/ocultar imagens



Para informações detalhadas, consulte a "Ajuda do inventário" na página 177.

Como ver propriedades de atributos

É possível visualizar as propriedades de atributo dos objetos Inventário de um dispositivo na listagem de inventários. As propriedades de atributo informam as características e os valores de um objeto do inventário. Também é possível criar novos atributos personalizados e editar os atributos definidos pelo usuário.

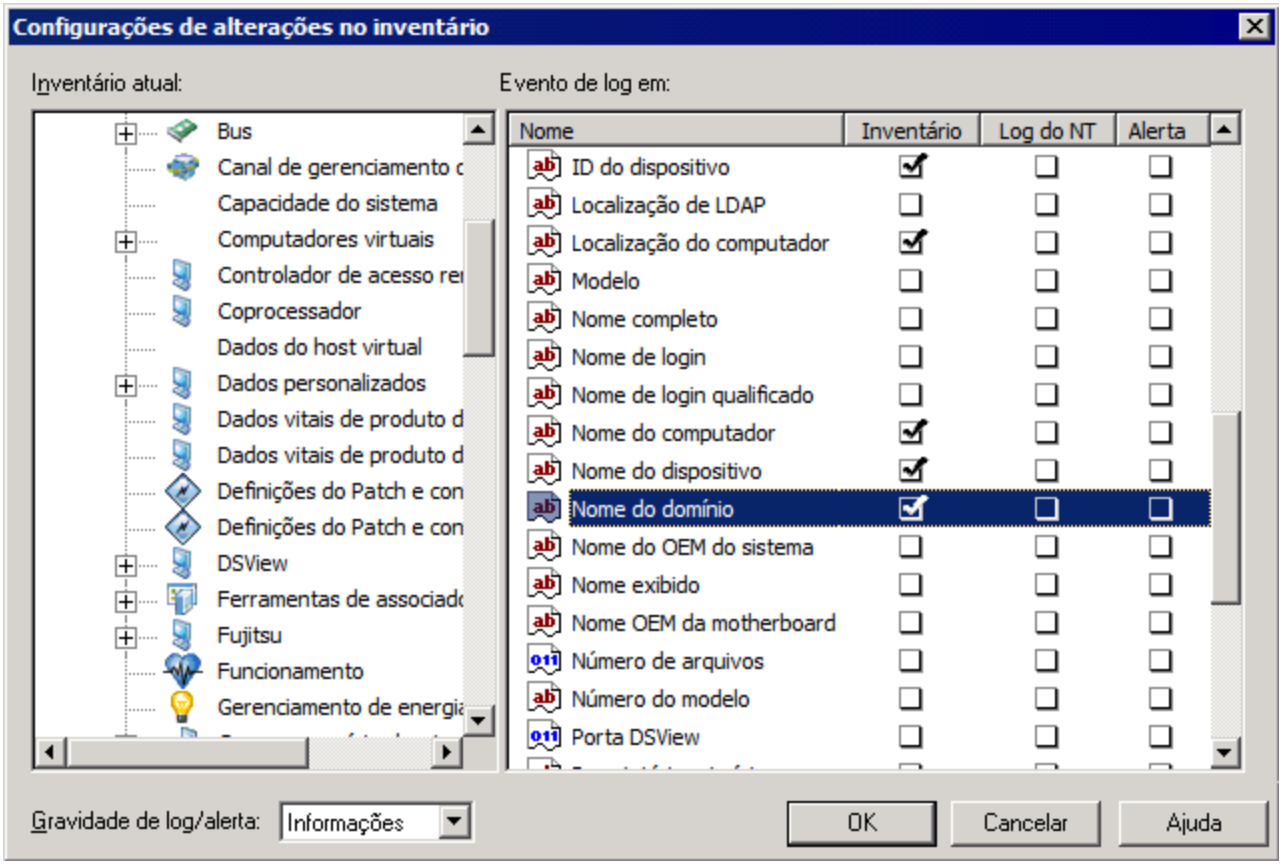
Para exibir as propriedades de um atributo, clique duas vezes no atributo.

Para obter mais informações, consulte a "Sobre a caixa de diálogo Propriedades do atributo de inventário" na página 179.

Controle das mudanças no inventário

LANDesk pode detectar e registrar mudanças no hardware e software do dispositivo. O controle das alterações no inventário pode ajudar a controlar os recursos da rede. As configurações de alteração no inventário permitem selecionar os tipos de alterações que você deseja salvar e com qual nível de gravidade. As alterações selecionadas podem ser salvas no log do histórico de inventário, log de eventos do Windows do servidor núcleo ou podem ser enviadas como um alerta AMS.

Exibir/ocultar imagens



É possível exibir e imprimir o histórico de alterações no inventário de um dispositivo. Além disso, é possível exportar as alterações no inventário para um arquivo .CSV formatado para análise usando suas próprias ferramentas de relatório.

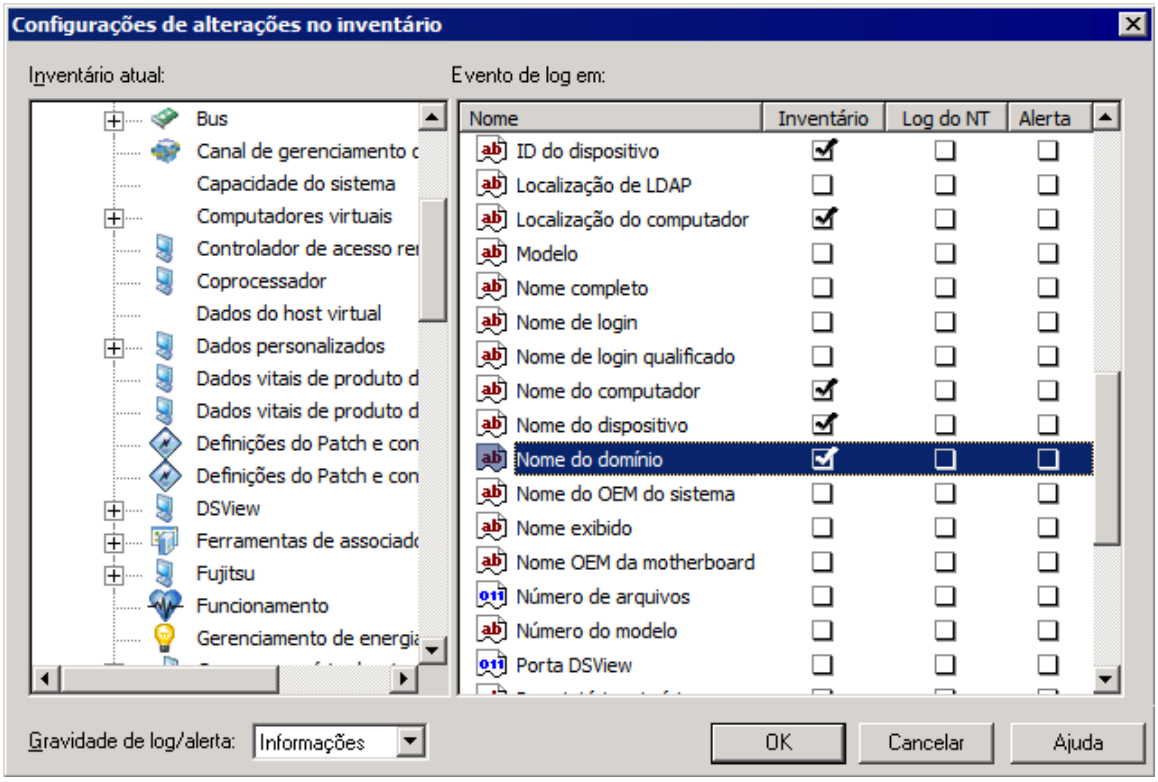
Para controlar e usar as alterações no inventário, primeiro é preciso definir as configurações de alterações no inventário. Você poderá realizar as outras tarefas do histórico de alterações no inventário:

- "Definir configurações de mudanças no inventário" na página 152
- "Exibição, impressão ou exportação das alterações no inventário" na página 153

Definir configurações de mudanças no inventário

NOTA: Você deve primeiro definir as configurações se desejar exibir, imprimir ou exportar as alterações no inventário de quaisquer dispositivos na rede.

Exibir/ocultar imagens



Para definir as configurações de mudanças no inventário

1. Clique em **Configurar** > **Histórico do inventário**.
2. Na caixa de diálogo **Configurações de alteração no inventário**, amplie o objeto **Computador** na lista **Inventários atuais** e selecione o componente de sistema que você deseja controlar.
3. Na lista **Registrar evento**, selecione o atributo do componente que deseja controlar.
4. Selecione a caixa de seleção apropriada para especificar onde registrar uma alteração no atributo em questão. As alterações no inventário podem ser registradas no log do histórico de alterações no inventário, log do visualizador de eventos do Windows NT ou como um alerta AMS.
5. Selecione um nível de gravidade na lista suspensa **Gravidade de log/alerta**. Os níveis de gravidade incluem: Nenhum, Informações, Aviso e Crítico.
6. Clique em **OK**.

Para obter mais informações, consulte a "Sobre a caixa de diálogo Configurações de alterações no inventário" na página 179.

Exibição, impressão ou exportação das alterações no inventário

Para exibir, imprimir ou exportar as alterações no inventário

1. Na tela de rede do console, clique com o botão direito do mouse em um dispositivo.
2. Clique em **Histórico do inventário**.

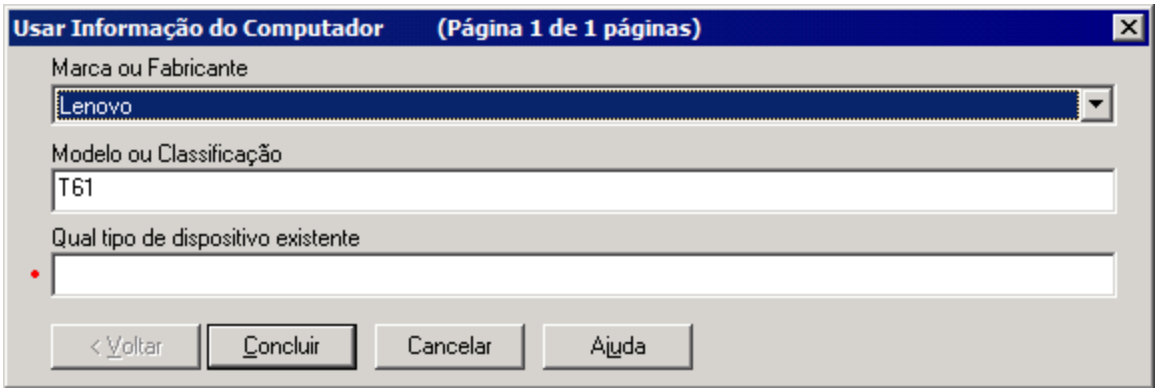
3. Clique em **Imprimir** para imprimir o histórico de alterações no inventário.
4. Clique em **Exportar** para salvar o histórico de alterações no inventário como um arquivo .CSV.

Para obter mais informações, consulte a "Sobre a caixa de diálogo Histórico de alterações no inventário" na página 180.

Uso de formulários de dados personalizados

A LANDesk inclui a ferramenta de formulários de dados personalizados (**Ferramentas** > **Formulários de dados personalizados**) que você pode usar para criar e gerenciar formulários. Os formulários de dados personalizados fornecem uma maneira de coletar informações de usuários e adicioná-las ao banco de dados núcleo.

Exibir/ocultar imagens



NOTA: O**LANDesk Security Suitenão oferece suporte à formulários de dados personalizados**
Os formulários de dados personalizados não estão indisponíveis somente com uma licença do LANDesk Security Suite. Você deve ter uma licença LANDesk Management Suite completa para usar o recurso de formulários de dados personalizados.

A varredura de inventário não pode coletar determinados tipos de informações personalizadas específicas do usuário, como:

- Localização da mesa de um usuário
- Número do ativo de um computador
- Número de telefone do usuário

A melhor maneira de obter essas informações é diretamente dos usuários com os formulários de dados personalizados.

Os formulários de dados personalizados têm dois componentes principais: o designer de formulários que é usado para criar formulários a serem preenchidos pelos usuários e a tela do formulário que é usada pelos usuários para o preenchimento dos formulários.

Os formulários podem ser armazenados central ou localmente. Se forem armazenados centralmente, todos os usuários terão acesso automático aos últimos formulários, pois todos poderão ver o mesmo formulário a partir do mesmo local. Se os formulários forem armazenados localmente, será preciso garantir que os usuários receberão os formulários mais recentes.

Após o usuário preencher um formulário, a tela de formulário armazenará os resultados localmente em C:\Program Files\LANDesk\LDClient\ldcstm.dat. Esse arquivo contém os resultados de todos os formulários aos quais o usuário respondeu. Se o usuário precisar preencher novamente o mesmo formulário (por exemplo, se o formulário original foi revisado), a Tela de formulário o preencherá com os dados anteriormente inseridos.

A varredura de inventário obtém as informações do arquivo LDCSTM.DAT de cada dispositivo e a adiciona ao banco de dados núcleo.

NOTA: Os bancos de dados Oracle diferenciam maiúsculas e minúsculas.
Ao criar campos personalizados com os formulários de dados personalizados (ou qualquer outro recurso) em um banco de dados Oracle, certifique-se de ter inserido os nomes dos campos com maiúsculas e minúsculas corretamente. Por exemplo, os dados associados a "Local do cubículo" são armazenados em um local diferente no banco de dados se comparados aos dados associados a "Local do Cubículo".

Além disso, certifique-se de que os campos personalizados tenham nomes que sejam exclusivos, independentemente da escrita em maiúsculas e minúsculas. Os dados corretos de inventário podem ser obtidos se dois campos personalizados tiverem o mesmo nome, mas tiverem sido digitados um em maiúsculas e outro em minúsculas.

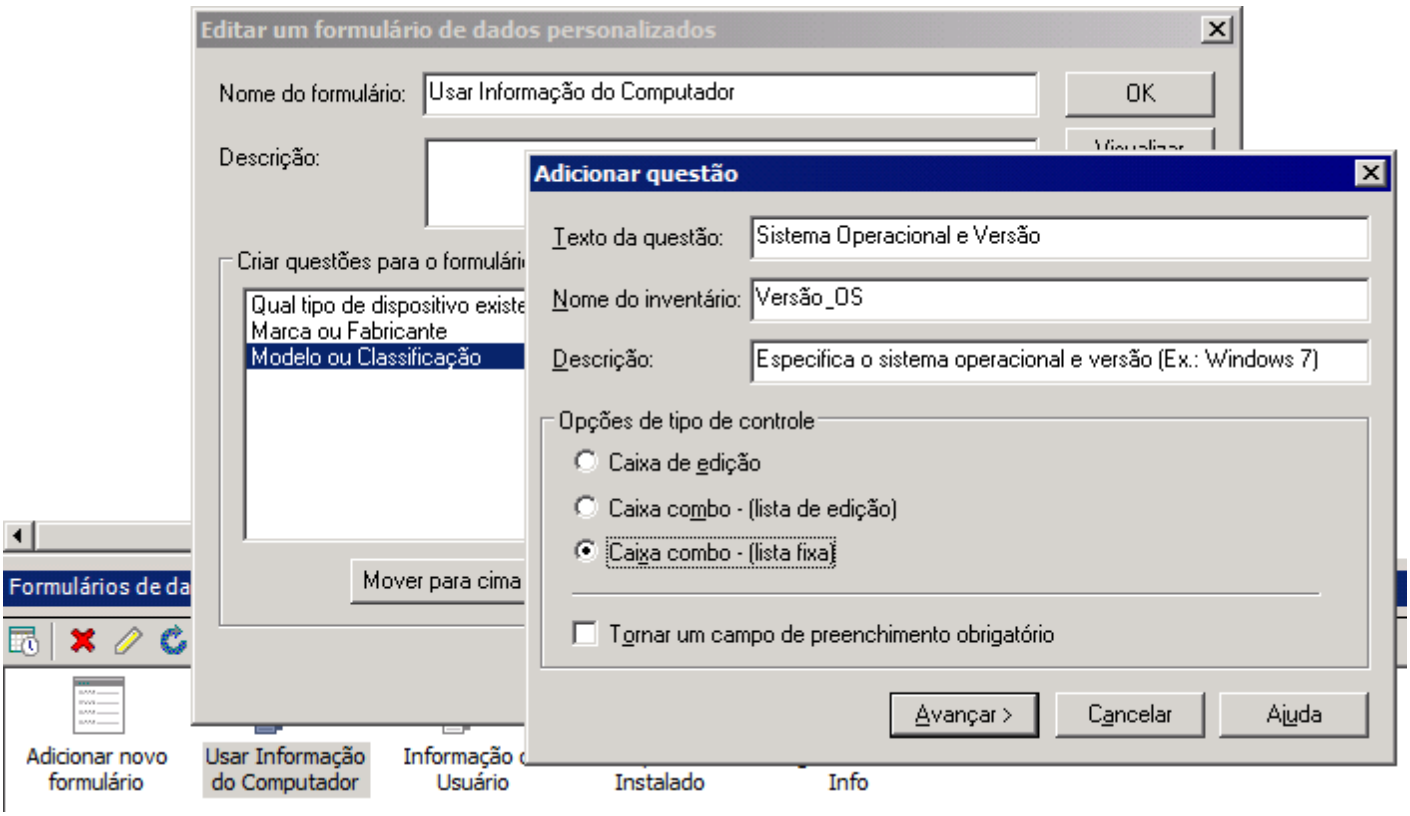
Criar um formulário de dados personalizados

Os formulários de dados personalizados fornecem uma maneira de coletar informações de usuários e adicioná-las ao banco de dados núcleo. Siga estas etapas para criar um formulário de dados personalizados.

Para criar um formulário de dados personalizados

1. Clique em **Ferramentas > Configuração > Formulários de dados personalizados**.
2. Na janela Formulários de dados personalizados, clique duas vezes em **Adicionar novo formulário**.
3. Digite um nome para o formulário.
4. Digite uma descrição para o formulário. (A descrição que você inserir será exibida como dica de Ajuda quando o usuário clicar F1 no campo, durante o preenchimento do formulário.)
5. Clique em **Adicionar** para abrir a caixa de diálogo **Adicionar pergunta**.
6. Na caixa de diálogo Adicionar pergunta, digite o **Texto da pergunta**, o **Nome do inventário** e a **Descrição.**
7. Selecione o **Tipo de controle**
8. Selecione se deseja que o campo seja obrigatório.
9. Se você tiver selecionado o tipo de controle **Editar**, clique em **Concluir** para fechar a caixa de diálogo **Adicionar pergunta**. O tipo de controle Editar permite que os usuários digitem suas próprias respostas às perguntas em uma caixa de texto editável. Você pode adicionar mais perguntas ou continuar na etapa 12.

Exibir/ocultar imagens



10. Se você tiver selecionado os dois tipos de controle **Caixa combo**, clique em **Avançar** para abrir a caixa de diálogo **Adicionar itens**. O tipo de controle Caixa combo permite que os usuários selecionem suas respostas em uma lista suspensa de itens predefinidos.
11. Na caixa de diálogo Adicionar itens, digite o nome de um item e clique em **Inserir** para colocá-lo na Lista de itens. Esses itens são exibidos em uma lista suspensa para essa pergunta do formulário. Você pode adicionar quantos itens desejar e, em seguida, clicar em **Concluir**.
12. Quando terminar de adicionar as perguntas, clique em **Fechar** para salvar o formulário.

Você pode clicar com o botão direito do mouse em um formulário para agendá-lo para distribuição aos dispositivos.

Criação de um grupo de formulários

Se você tiver mais de um formulário que deseja enviar aos dispositivos, poderá organizá-los em um grupo. Em seguida, você poderá simplesmente agendar o grupo de formulários para distribuição.

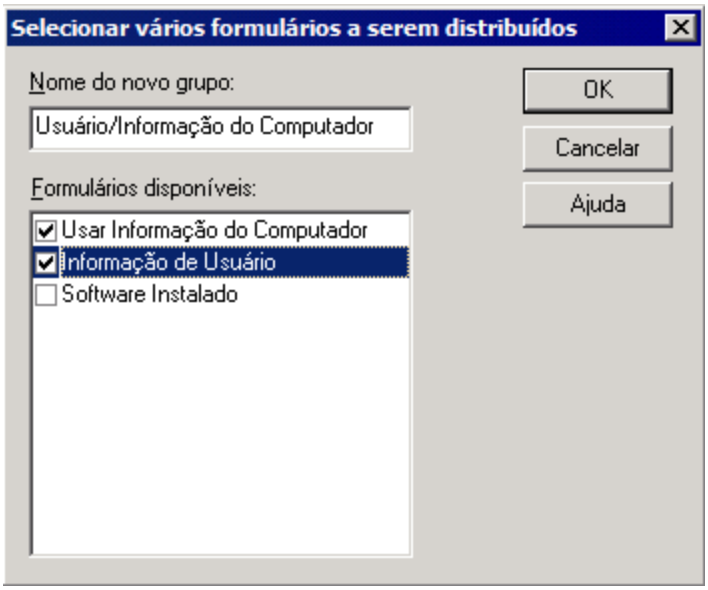
Ao agendar um grupo de formulários para distribuição, o agendador local lê o conteúdo do grupo quando for o momento da distribuição. Em outras palavras, você ainda pode alterar o conteúdo do grupo mesmo depois de agendado (desde que a tarefa agendada ainda não tenha ocorrido).

NOTA: Se um formulário que faça parte de um grupo for posteriormente modificado ou excluído, o grupo refletirá automaticamente essas alterações.

Para criar um grupo de formulários

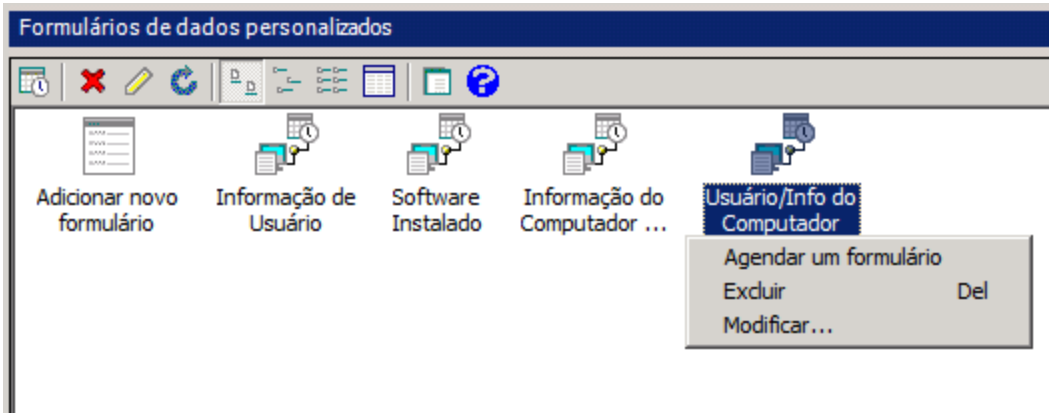
1. Na janela **Formulários de dados personalizados**, clique no botão da barra de ferramentas **Múltiplos formulários.**
2. Digite um nome para o novo grupo.
3. Selecione os formulários que deseja adicionar ao grupo na lista de formulários disponíveis.
4. Clique em **OK**.

Exibir/ocultar imagens



Após criar um grupo de formulários, você pode clicar com o botão direito do mouse em um grupo de formulários para agendá-lo para distribuição aos dispositivos.

Exibir/ocultar imagens



Configuração de dispositivos que receberão formulários de dados personalizados

Ao configurar dispositivos, será possível configurá-los para receber formulários de dados personalizados. Você deve selecionar a instalação do componente formulários de dados personalizados, e especificar as opções nas páginas do formulário de dados personalizados da caixa de diálogo Configuração do cliente. Para obter mais informações, consulte a "Distribuindo formulários de dados personalizados" na página 119.

Na caixa de diálogo configuração do agente, especifique a forma como deseja atualizar os formulários no dispositivo:

- **Atualização automática:** Se todos os formulários forem armazenados centralmente (atualizações automáticas), os usuários selecionarão um único local para novos formulários. Dessa maneira, quando um novo formulário estiver disponível, todos os dispositivos terão acesso imediato a ele. A desvantagem é que os usuários podem ver os formulários que não são relevantes a eles.
- **Atualização manual:** Se os formulários forem armazenados localmente (atualizações manuais), você precisará distribuí-los aos usuários que precisarem preenchê-los. Haverá menos sobrecarga na rede já que cada dispositivo terá sua própria cópia do formulário. O benefício dos formulários locais é que você pode limitar os formulários que os usuários verão apenas aos que são relevantes a eles. Você copia os formulários para os dispositivos durante a configuração do dispositivo ou com a ferramenta Tarefas agendadas.

Também é necessário especificar quando os formulários serão mostrados no dispositivo:

- **Na inicialização:** A Tela de formulário do cliente verifica se há formulários novos ou modificados sempre que o cliente inicializar. Ela será iniciado após o sistema operacional ser carregado. Na próxima vez em que a varredura de inventário for executada, ela enviará formulários preenchidos ao banco de dados núcleo.
- **Quando a varredura de inventário for executada:** Ela iniciará a Tela de formulário, que verificará se há formulários novos ou modificados. Assim que os usuários terminarem de preencher o formulário e fecharem a Tela de formulário, a varredura será concluída e os dados serão inseridos no banco de dados núcleo.
- **Quando iniciado a partir da pasta de programas do LANDesk:** A Tela de formulário pode ser iniciada manualmente no grupo de programas do Management Suite. Na próxima vez em que a varredura de inventário for executada, ela enviará formulários preenchidos ao banco de dados núcleo.

Você pode também usar a janela **Tarefas agendadas** para disparar a Tela de formulário em dispositivos em horários predefinidos. Neste cenário, use a janela **Tarefas agendadas** para, primeiramente, distribuir o formulários aos dispositivos. Certifique-se de atribuir tempo suficiente para distribuir os formulários antes de usar o recurso das tarefas de script de tarefas agendadas para executar a Tela de formulário.

Preenchimento de formulários no dispositivo

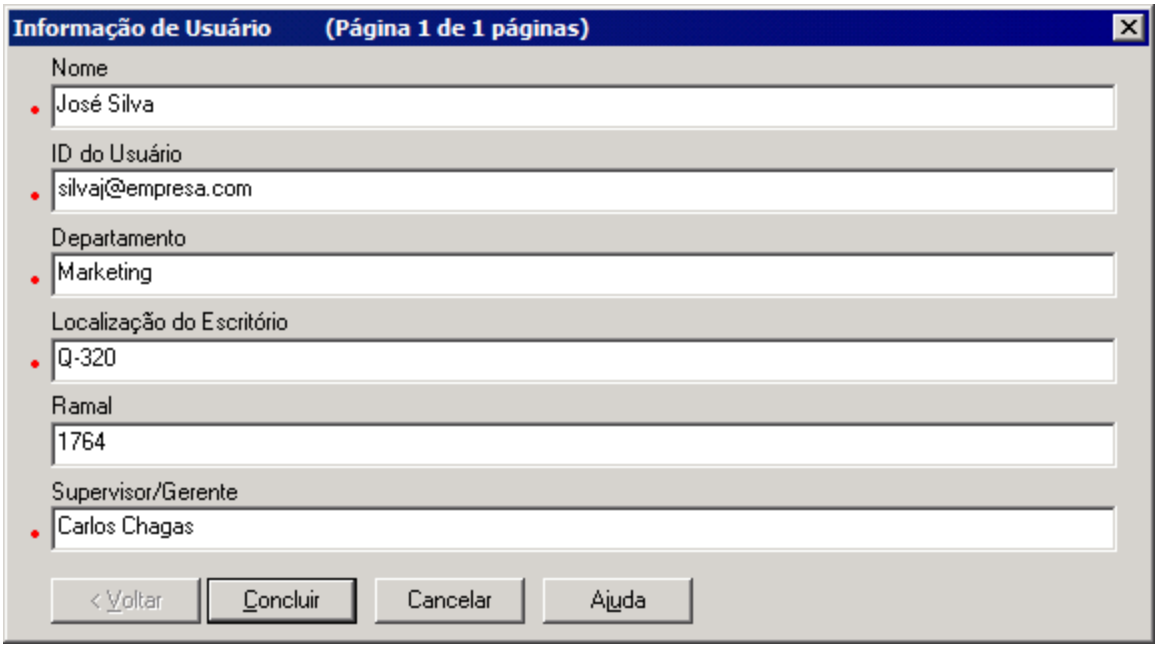
IMPORTANTE: Você pode agendar formulários de dados personalizados (ou grupos de formulários) para distribuição para dispositivos usando a ferramenta Tarefas agendadas (**Distribuição > Tarefas agendadas**). Antes da exibição de formulários no dispositivo, talvez seja necessário que você ative a exibição de formulários na ferramenta de Configuração de agente (**Configuração > Configuração de agente > (clique duas vezes na configuração aplicável na lista) > Formulários de dados personalizados >selecione a opção de exibição que você deseja usar**).

Quando a Tela de formulário for iniciada no dispositivo, uma lista de formulários e o status de cada um serão exibidos:

- **Novo:** Indica que o formulário nunca foi preenchido pelo usuário.
- **Concluído:** Indica que o usuário abriu o formulário e preencheu, no mínimo, os campos obrigatórios.
- **Refazer:** Indica que o usuário preencheu o formulário anteriormente, mas, desde então, ele foi alterado. O usuário precisa acessar novamente o formulário e fazer as alterações necessárias. Uma vez isso feito, o status do formulário é alterado para concluído.

Quando os usuários selecionam um formulário para preenchimento e clicam em **Abrir**, um assistente simples de Formulários é exibido. Ele contém uma lista de perguntas e campos para respostas. Se existirem mais perguntas do que caibam em uma página, também existirão os botões Voltar/Avançar. Os usuários podem clicar em **Ajuda** (ou pressionar **F1**) enquanto o cursor estiver em um campo para exibir uma mensagem de ajuda gerada pelo campo **Descrição** no designer de formulários.

Exibir/ocultar imagens

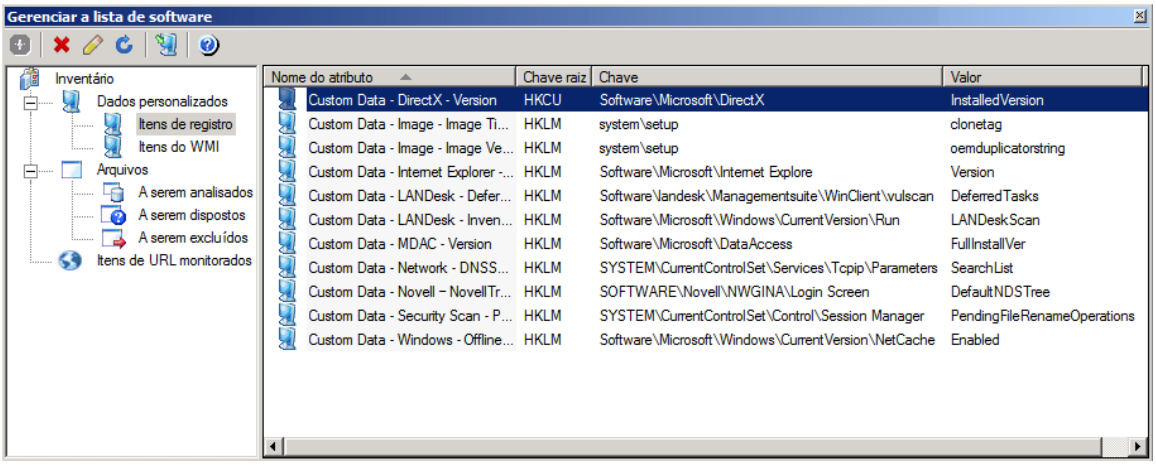


Os usuários devem responder a todas as perguntas necessárias antes de continuar na página seguinte ou sair de um formulário. As perguntas obrigatórias têm um ponto vermelho ao lado.

A última página do assistente de Formulários contém um botão **Concluir** que os usuários clicam quando tiverem terminado. Ao clicarem nesse botão, os usuários retornarão à caixa de diálogo **Seleção de formulários**, na qual a mensagem de status ao lado do nome do formulário é atualizada.

Adicionar softwares e dados às análises de inventário

Use a ferramenta **Gerenciar lista de softwares** para configurar os softwares e os dados que você deseja incluir nas análises de inventário. As escolhas que você faz com essa ferramenta determina quais itens serão analisados quando o analisador de inventário for executado.



O analisador de inventário usa os itens de dados que você especificar para identificar arquivos de software e de itens de dados personalizados, como valores de registro, dados do WMI e URLs. É possível especificar os seguintes itens:

- **Arquivos:** Os arquivos que se encontram incluídos nas análises de software estão incluídos na lista **A serem analisados**. Arquivos na lista **A serem excluídos** não são incluídos nas análises de software. Os arquivos na lista **A serem dispostos** foram descobertos e precisam ser movidos para uma das outras listas.
- Itens de registro: O analisador de inventário pode identificar itens no registro do Windows nos dispositivos gerenciados. Estes itens são exibidos na secção da lista de inventário que você especificar.
- Itens do WMI: O analisador de inventário pode buscar por itens de dados de WMI (Windows Management Instrumentation) e apresentar os resultados na seção da lista de inventário que você especificar.
- **URLs**: O analisador de inventário pode procurar URLs, o que é útil para rastrear o uso de aplicativos baseados na Web e de software como um serviço (SaaS).

Consulte os tópicos a seguir para obter informações sobre alteração de itens incluídos em análises de inventário:

- "Adicionar ou remover arquivos para análises de inventário" na página 160
- "Adicionar itens de registro personalizados nas análises de inventário" na página 162
- "Adicionar itens de WMI personalizados nas análises de inventário" na página 164
- "Adicionar URLs às análises de inventário" na página 165

Adicionar ou remover arquivos para análises de inventário

Modifique os arquivos na ferramenta Gerenciar lista de softwares para determinar quais arquivos são incluídos ou excluídos das análises.

NOTA: Após alterar qualquer item em Gerenciar lista de softwares do core, você deve clicar no botão **Disponibilizar para clientes** para atualizar os arquivos de definição do produto usado pelo analisador de inventário. A próxima vez que os dispositivos realizarem uma análise de inventário, a varredura obtém os arquivos de definição de produto atualizados do servidor núcleo e aplica as mudanças.

Arquivos de software em análises de inventário

A varredura identifica os aplicativos do software de três formas:

- Nome do arquivo
- Nome e tamanho do arquivo
- informações contidas em um arquivo executável do aplicativo.

Use o modo de exibição de árvore do **Gerenciar lista de softwares** para especificar quais arquivos devem ser analisados e quais devem ser excluídos da análise do inventário. O item **Arquivos** na árvore exibe três categorias que ajudam na organização dos arquivos:

- **A serem analisados:** Arquivos que o analisador identificará nos dispositivos. Esta lista é pré-povoada com descrições de diversos aplicativos, fornecendo uma base dos executáveis que podem ter sido instalados nos dispositivos. Você pode adicionar ou excluir arquivos dessa lista.
- **A serem dispostos:** O analisador de inventário adiciona dados de software à base de dados, ele encontra muitos arquivos de software que não são reconhecidos; esses arquivos são adicionados a esta lista. Você pode mover os arquivos desta lista para qualquer das outras duas listas.
- **A serem excluídos:** O analisador ignora todas as ocorrências de todos os arquivos movidos para cá. Se você excluir um arquivo de **A serem excluídos**, ele aparecerá na categoria **A serem dispostos**.

Como padrão, a análise do inventário só analisa arquivos encontrados em Gerenciar lista de softwares. Os arquivos especificados como analisados ou excluídos são gravados no arquivo de configuração do inventário.

Se quiser analisar todos os arquivos nos dispositivos, você pode mudar o modo de análise para todos os arquivos. Analisar todos os arquivos pode gerar arquivos de análise de inventário com vários megabytes. Depois da análise inicial, a análise do inventário envia somente análises delta, que são muito menores.

Para obter mais informações sobre como alterar o modo de análise, e uma descrição do arquivo de configuração do inventário, consulte "Editar o arquivo LdAppl3.Template file" na página 168 .

Analise ou exclua arquivos de software

Complete as seguintes tarefas para determinar quais arquivos de software estão incluídos na analise de inventário.

Para incluir um arquivo nas análises de inventário:

1. Localize o arquivo na lista **A serem dispostos**.
2. Arraste o arquivo para a lista **A serem analisados**.

Para excluir um arquivo das análises de inventário

1. Localize o arquivo na lista **A serem dispostos**.
2. Arraste o arquivo para a lista **A serem excluídos**.

Para excluir um arquivo não encontrado na lista A serem dispostos

1. Clique me **A serem excluídos** e clique no botão **Adicionar** da barra de ferramentas.
2. Digite o nome do arquivos a ser excluído e clique em **OK**.

Para alterar o status de um arquivo de analisado para excluído

1. Localize o arquivo pesquisando na lista **A serem analisados**.
2. Arraste o arquivo para a lista **A serem excluídos**.

Você também pode mover os arquivos da lista excluída para lista de analisados.

Analisar arquivos de aplicativos sem extensões .exe

Como padrão, a lista **A serem analisados** contém descrições de executáveis, mas somente com arquivos de extensões .exe. Se quiser que o analisador identifique também outros tipos de arquivos de aplicativos (.dll, .com, .sys e assim por diante), consulte "Editar o arquivo LdAppl3.Template file" na página 168.

Sobre a caixa de diálogo Propriedades do arquivo

Use esta caixa de diálogo para adicionar arquivos em Gerenciar lista de softwares.

- **Botão Procurar:** use esse botão para selecionar diretamente um arquivo. A opção de selecionar um arquivo desta maneira preencherá os campos Nome do arquivo e Tamanho para você.
- **Nome do arquivo:** Procure ou digite um nome de arquivo.
- **Tamanho (em bytes):** insira o tamanho do arquivo em bytes. Não use vírgula ou outros separadores entre os dígitos. Se digitar arquivo de tamanho o 1, qualquer arquivo com esse nome corresponderá.
- **Nome do produto:** insira o nome do produto ao qual o arquivo pertence.
- **Fornecedor:** digite o nome do fornecedor do produto que usa o arquivo.
- **Versão:** digite o nome da versão do arquivo.
- **Ação ou estado:** selecione o que você deseja fazer com o arquivo:
  - **A serem analisados:** adicione o arquivo a esta categoria para a varredura de inventário procurar por ele nos dispositivos.
  - **A serem dispostos:** Adicione o arquivo a esta categoria se desejar decidir posteriormente o que deseja fazer com o arquivo.

Adicionar itens de registro personalizados nas análises de inventário

O analisador de inventário pode analisar as chaves do registro especificadas e adicionar os valores no banco de dados núcleo. Esse processo pode ser útil para o software personalizado, as informações de recursos ou outras informações armazenadas no registro que você deseja incluir no banco de dados núcleo.

A ferramenta Gerenciar software permite que você especifique as chaves de registro que serão adicionadas à analise de inventário. Os resultados são exibidos em qualquer secção do inventário que você especificar.

Vários itens de registro são fornecidos com Management Suite. Você pode exibir as propriedades desses itens para ver um exemplo de como criar itens de registro. Para ver as propriedades de um item, clique nele com o botão direito do mouse e selecione **Propriedades**.

Para adicionar uma chave de registro na analise de inventário

1. Clique em **Ferramentas > Relatórios/Monitoração > Gerenciar lista de softwares**.
2. Expanda **Dados personalizados** e clique em **Itens de registro**.
3. Clique no botão **Adicionar** na barra de ferramentas.

4. Selecione e insira os dados conforme descrito abaixo.
5. Clique em **OK**.

Itens de análise de registro incluem os dados a seguir:

- **Chave da raiz**: Selecione o tipo de chave de registro que deseja analisar.

  HKLM = HKEY_LOCAL_MACHINE

  HKCC = HKEY_CURRENT_CONFIG

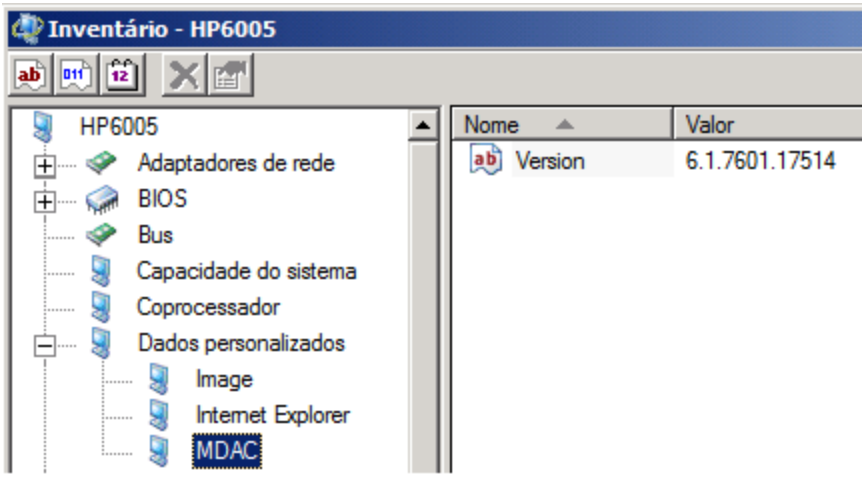
  HKCR = HKEY_CLASSES_ROOT

  HKU = HKEY_USERS

  HKCU = HKEY_CURRENT_USER

- **Chave:** O caminho do registro que define o local da chave. Os itens devem ser separadas com uma barra invertida (\ ), e cada item entre barras representa um nível na hierarquia de árvore do registro (como exibido no editor de registro).
- **Valor:** O valor da pesquisa que o analisador de inventário procura.
- **Nome do atributo:** A descrição do local onde os dados serão exibidos na árvore de inventário. Os itens estão listados em ordem hierárquica e devem ser separados com " - " (espaço-hífen-espaço) para ser exibido de forma precisa no inventário. O primeiro item que você deve digitar aqui é o nome da árvore do inventário que conterá os dados, por exemplo, "Dados personalizados".

  Por exemplo, o nome do atributo `Dados personalizados - MDAC - Versão` é exibido em um resumo de inventário do dispositivo como a seguir:



NOTA: Após alterar qualquer item em Gerenciar lista de softwares do core, você deve clicar no botão **Disponibilizar para clientes** para atualizar os arquivos de definição do produto usado pelo analisador de inventário. A próxima vez que os dispositivos realizarem uma análise de inventário, a varredura obtém os arquivos de definição de produto atualizados do servidor núcleo e aplica as mudanças.

Adicionar itens de WMI personalizados nas análises de inventário

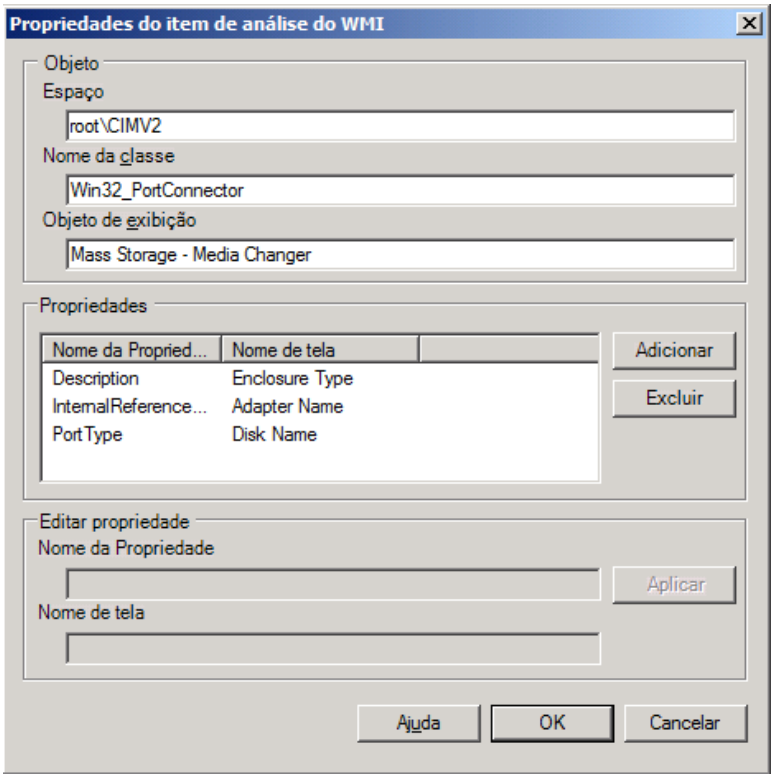
O analisador de inventário pode analisar dados do WMI (Windows Management Instrumentation) as adicionar seus valores ao banco de dados do núcleo. Esses dados são exibidos no resumo do inventário.

Use esta opção se existirem itens de inventário de dispositivos do Windows que você não consegue encontrar no resumo de inventário fornecido com o Management Suite.

Para adicionar itens de WMI a análise de inventário, você deve estar familiarizado com as classes e instâncias do WMI, e precisará saber de qual 'namespace' uma classe faz parte. Use uma ferramenta como Microsoft CIM Studio ou PowerShell (no Windows 7) para procurar as classes WMI.

Para cada classe, você pode analisar uma ou mais propriedades e devolver esses valores na árvore de inventário.

A seguir, um exemplo de classe de WMI para um conector de porta de comunicação. Ela contém três propriedades. O namespace, classe e o caminho de exibição do inventário são definidos na seção superior da caixa de diálogo. As propriedades são adicionadas individualmente e são todas listadas na caixa de propriedades no meio da caixa de diálogo.



Após definir e disponibilizar este item de dado personalizado a dispositivos gerenciados (clicando em **Tornar disponível para os clientes** na barra de ferramentas), um dispositivo gerenciado com conector de porta de comunicação incluirá esse item no resumo do inventário. Na árvore do inventário, o item é listado em Armazenamento de massa > Trocador de mídia. Ele exibirá três itens de dados: Nome do adaptador, Nome do disco e Tipo de compartimento.

Para adicionar um item do WMI na analise de inventário

1. Clique em **Ferramentas > Relatórios/Monitoração > Gerenciar lista de softwares**.
2. Expanda **Dados personalizados** e clique em **Itens de WMI**.
3. Clique no botão **Adicionar** na barra de ferramentas.
4. Digite os dados do **Objeto**, conforme descrito abaixo.
5. Para adicionar uma propriedade, clique em **Adicionar**. Digite um **Nome de propriedade** e um **Nome de tela** como descrito abaixo. Clique em **Aplicar** para adicionar as propriedades.
6. Quando todas os dados forem preenchidos, clique em **OK**.

Itens de WMI incluem os seguintes dados:

- **NameSpace**: O espaço de nome de WMI. Normalmente, é `root\\CIMV2`, mas pode ser outro namespace.
- **Nome da classe**: O nome da classe de WMI.
- **Objeto de exibição**: A descrição do local onde os dados serão exibidos na árvore de inventário. Os itens estão listados em ordem hierárquica e devem ser separados com " - " (espaço-hífen-espaço) para ser exibido de forma precisa no inventário. O primeiro item que você deve digitar aqui é o nome da árvore do inventário que conterá os dados, por exemplo, "Dados personalizados".

Cada item pode ter uma ou mais propriedades que o analisador busca.

- **Nome da propriedade**: O nome que identifica a propriedade de WMI.
- **Nome de exibição:** O nome utilizado na árvore de inventário para identificar a propriedade de WMI. Este nome aparece um nível abaixo do objeto de exibição na árvore do inventário.

NOTA: Após alterar qualquer item em Gerenciar lista de softwares do core, você deve clicar no botão **Disponibilizar para clientes** para atualizar os arquivos de definição do produto usado pelo analisador de inventário. A próxima vez que os dispositivos realizarem uma análise de inventário, a varredura obtém os arquivos de definição de produto atualizados do servidor núcleo e aplica as mudanças.

Adicionar URLs às análises de inventário

O analisador de inventário pode procurar URLs, o que é útil para rastrear o uso de aplicativos baseados na Web e de software como um serviço (SaaS).

Para cada URL que você adicionar, o analisador de inventário irá salvar os tipos de dados a seguir:

- Frequência de visitação do URL
- Tempo gasto na visualização de páginas no URL
- A última data/hora que o URL foi visitado

Para adicionar um URL na analise de inventário

1. Clique em **Ferramentas > Relatórios/Monitoração > Gerenciar lista de softwares**.
2. Clique em **Itens de URL monitorados**.
3. Clique no botão **Adicionar** na barra de ferramentas.
4. Insira um nome de domínio na caixa de URL.

Você pode inserir um nome de domínio com subdomínios, separados por pontos, mas você não pode incluir caminhos específicos. O nome do domínio não pode conter caracteres inválidos. Se você inserir um caminho ou caracteres inválidos, uma mensagem de erro sera exibida e você terá de corrigir a URL.

Você pode incluir até 10 níveis de subdomínios com no máximo 60 caracteres por nível. Você pode usar um máximo de 260 caracteres no nome de domínio.

NOTA: Após alterar qualquer item em Gerenciar lista de softwares do core, você deve clicar no botão **Disponibilizar para clientes** para atualizar os arquivos de definição do produto usado pelo analisador de inventário. A próxima vez que os dispositivos realizarem uma análise de inventário, a varredura obtém os arquivos de definição de produto atualizados do servidor núcleo e aplica as mudanças.

Alteração dos parâmetros da análise de inventário

Este tópico descreve as diferentes formas de alterar os parâmetros de análises de inventário. Também inclui as seguintes informações:

- "Análise de informações personalizadas" na página 166
- "Especificação do intervalo e histórico da análise de software" na página 167
- "Parâmetros da linha de comando do analisador" na página 167
- "Editar o arquivo LdAppl3.Template file" na página 168
- "Adição de sequências de texto do BIOS ao banco de dados do núcleo" na página 170

Análise de informações personalizadas

O utilitário analisador de inventário do Windows faz uma varredura no registro do dispositivo a procura de informações personalizadas. Quando um dispositivo é configurado, as seguintes chaves são instaladas no registro:

- HKEY_LOCAL_MACHINE\SOFTWARE\INTEL\LANDESK\INVENTORY\CUSTOM FIELDS

O analisador de inventário sempre analisa a chave Custom Fields do registro e seleciona as informações encontradas nessa chave. Em seguida, insere as informações personalizadas em Campos Personalizados no banco de dados núcleo. As informações nas chaves de Campos personalizados podem ser o que você quiser. Quando esses dados são examinados no console, eles são exibidos em Campos Personalizados.

O analisador de inventário faz a leitura de dois tipos de dados:

- REG_SZ
- REG_DWORD

NOTA: Subchaves de Campo personalizado
A análise de inventário não analisa nenhuma subchave abaixo de Campos personalizados.

NOTA: Tamanho da seqüência de caracteres de Campos personalizados
As seqüências de caracteres ASCII não devem ultrapassar 255 caracteres. As seqüências de caracteres MBCS (Multi-byte Character Set, Conjunto de caracteres de bytes múltiplos) devem conter entre 127 e 255 caracteres.

Especificação do intervalo e histórico da análise de software

É possível especificar o momento da análise de software do dispositivo e com que freqüência salvar o log de histórico das alterações no inventário no servidor núcleo. Esses intervalos aplicam-se a cada dispositivo.

NOTA: O *hardware* de um dispositivo será analisado sempre que ele for inicializado e estiver conectado à rede.

Para especificar as configurações de análise de software

1. Na tela de rede do console, clique em **Configurar > Serviços > Inventário > Software**.
2. Especifique a freqüência de análise de software.
3. Especifique o número de dias para salvar o histórico.

NOTA: Análise do servidor núcleo e do software
Esse recurso afeta somente os dispositivos. Não afeta o servidor núcleo, que é analisado diariamente.

Parâmetros da linha de comando do analisador

Você pode adicionar parâmetros de linha de comando às propriedades do atalho (ldiscn32.exe) do analisador de inventário para controlar como ela funciona.

A seguinte tabela relaciona os parâmetros de linha de comando do analisador:

Opção	Descrição
/NTT=IP	Endereço IP do servidor núcleo ou nome DNS e porta UDP. Por exemplo, /NTT=123.123.123.123:5007 ou /NTT=CORESERVER:5007.
/UDP	O analisador comunica-se por meio de UDP em vez de TCP. Combine essa chave com /NTT=[IP].
/NOUI	Força o analisador a ser executado sem interface com o usuário.
/i=inifile	Fornece o caminho (HTTP, UNC) ou uma letra da unidade) ao arquivo principal LdAppl3.O ldiscn32.exe também copia o arquivo LdAppl3 encontrado neste local no arquivo localLdAppl3.ini do dispositivo. Os analisadores comparam as datas do LdAppl3 principal com as do LdAppl3.ini local; se elas não forem iguais, o arquivo principal será copiado localmente.
/d=directory	Inicia a análise de software no diretório especificado. Por padrão, a análise é iniciada no diretório raiz de cada disco rígido local.
/L	Envia a análise para o servidor núcleo do qual o dispositivo foi configurado. Quando você usa /L, o parâmetro /NTT não é necessário.

Opção	Descrição
/sync	Força uma análise completa, inclusive uma análise completa do software. Os arquivos com análise completa podem ter vários megabytes de tamanho.
/n	Não pesquisa subdiretórios.
/v	Modo de detalhes.
/Z=retry count	Especifica quantas vezes o analisador tenta enviar novamente a análise.
/W=espera em segundos	Tempo de espera especificado em segundos que o analisador aguardou antes de iniciar uma análise.
/? or /h	Exibe a ajuda de sintaxe da linha de comando.
/s=servername	Especifica o servidor núcleo no qual armazenar os dados de inventário.
/f ou /f-	Força uma análise de software, independente do intervalo de análise de software definido no console. Especifique /f- para desativar a análise de software independente do intervalo de análise de software definido no console.
/t=[path] filename	Copia o conteúdo do arquivo especificado para o banco de dados núcleo. Use essa opção para inserir dados de inventário de dispositivos independentes ou de arquivos de inventário separados.
/o=[path] filename	Grava os dados de inventário no arquivo de saída especificado.
/m	Cria um arquivo ldiscan.mif não-unicode no diretório C:/DMI/DOS/MIFS. Esse arquivo contém os dados de inventário localizados durante a análise.
/muni	(Somente ldiscn32.exe) Cria um arquivo ldiscan.mifunicode no diretório localizado em MIFPATH do arquivo LdAppl3.ini. Esse arquivo contém os dados de inventário localizados durante a análise.
/do16	Habilita a análise de inventário de 16 bits (inv16.exe) nos dispositivos gerenciados.

Editar o arquivo LdAppl3.Template file

Informações sobre os parâmetros de inventário do analisador estão contidas no arquivo LdAppl3.Template. Esse arquivo de modelo trabalha com o arquivo LdAppl3 para identificar o inventário de software de um dispositivo.

Você pode editar a seção [LANDesk Inventory] do arquivo modelo para configurar os parâmetros que determinam como o analisador identifica o inventário de software. Por padrão, o LdAppl3.Template está localizado no diretório do servidor núcleo:

- \Arquivos de programas\LANDesk\ManagementSuite\LDLogon

Use esta tabela como um como guia para ajudar a editar a seção [LANDesk Inventory] em um editor de texto.

Opção	Descrição
Modo	Determina como o analisador examina o software nos dispositivos. O padrão é Listed. As configurações são as seguintes: • **Listado:** Registra os arquivos listados em LdAppl3. • **Não listado:** Registra os nomes e as datas de todos os arquivos com as extensões listadas na linha ScanExtensions, mas que não foram definidas no LdAppl3. Esse modo ajuda a descobrir o software não autorizado na rede. • **Todos:** Descobre arquivos com extensões contidas na linha ScanExtensions.
Duplicados	Registra instâncias múltiplas de arquivos. Defina o valor como OFF para registrar apenas a primeira instância ou como ON para registrar todas as instâncias detectadas. O padrão é ON.
ScanExtensions	Define as extensões dos arquivos (.exe, .com, .cfg etc.) a serem analisados. Use um espaço para separar as extensões de arquivos. Por padrão, apenas arquivos .exe são analisados.
Versão	É o número da versão do arquivo LdAppl3.
Revisão	É o número de revisão do arquivo LdAppl3; ajuda a garantir a compatibilidade futura.
CfgFiles 1-4	Registra a data, a hora, o tamanho e o conteúdo dos arquivos especificados. Você pode omitir a letra da unidade (por exemplo, c:) se quiser que a pesquisar todas as unidades físicas. É possível especificar mais de um arquivo em cada uma das quatro linhas, mas o tamanho da linha é limitado a 80 caracteres. Separe os nomes de caminho contidos na mesma linha com um espaço. A análise compara a data e o tamanho do arquivo atual com o arquivo analisado anteriormente. Se a data e o tamanho forem diferentes, a análise registrará o conteúdo do arquivo como uma nova revisão.
ExcludeDir 1-3	Exclui os diretórios específicos de uma análise. Você pode omitir a letra da unidade (por exemplo, c:) se quiser excluir todas as unidades físicas. A enumeração deve começar no 1 e ser contínua. Use as variáveis de ambiente no formato: "%varname%". Use um curinga (*) somente em "começa com" (ExcludeDir=%windir%\$NtUninstall*\ ). Cada linha deve terminar com "\".
MifPath	Especifica o local no qual os arquivos MIF estão armazenados em uma unidade local do dispositivo. O local padrão é c:\DMI\DOS\MIFS.

Opção	Descrição
UseDefaultVersion	Se definido como VERDADEIRO, o analisador informará quando um arquivo corresponder a uma entrada exata de nome e tamanho do arquivo em LdAppl3 somente no nome do arquivo (a versão será reportada como EXISTS). Isso pode causar alguns falsos positivos para aplicativos que compartilham um nome de arquivo comum com um aplicativo desconhecido. No arquivo original LdAppl3.Template, esse parâmetro é definido como FALSO; ou seja, uma entrada será adicionada apenas se a correspondência for exata. Se o parâmetro não estiver presente, ele assumirá TRUE como padrão.
SendExtraFileData	Se definido como TRUE, envia dados adicionais do arquivo para o servidor núcleo. O padrão é FALSE. Isso significa que, por padrão, apenas o caminho, o nome e a versão serão inseridos no banco de dados núcleo.

Disponibilização das mudanças na análise de inventário para clientes

Ao fazer mudanças no arquivo LdAppl3.template, você precisa distribuir as mudanças para os dispositivos gerenciados para mudar a forma de execução das análises de inventário. As mudanças serão aplicadas se o parâmetro i/ da linha de comando do analisador for utilizado nos dispositivos gerenciados.

Para editar o arquivo LdAppl3.Template

1. No servidor núcleo, vá para o diretório LDLogon e abra o LdAppl3.Template no bloco de notas ou em outro editor de texto.
2. Use a barra de rolagem para chegar no parâmetro que deseja atualizar e faça as modificações.
3. Salve o arquivo.

Para distribuir mudanças aos dispositivos gerenciados

1. Edite e salve o arquivo LdAppl3.Template.
2. No console, clique em **Ferramentas > Relatórios/Monitoramento > Gerenciar lista de softwares**.
3. Clique no botão **Disponibilizar aos clientes** da barra de ferramentas para tornar as mudanças mais recentes disponíveis aos dispositivos na próxima vez que executarem uma análise de inventário.

Adição de sequências de texto do BIOS ao banco de dados do núcleo

Há uma seção no arquivo LdAppl3.Template denominada [BIOS Info]. Essa seção fornece o recurso de pesquisa de informações dentro do BIOS de um computador. Você pode adicionar uma ou mais entradas à seção [BIOS Info]. Essas entradas definem novas chaves no banco de dados núcleo e fornecem instruções de análise para o analisador de inventário. As instruções de análise identificam onde procurar uma seqüência específica no arquivo LDBIOS.TXT. Usando essas instruções, o analisador de inventário preenche o banco de dados núcleo com seqüências do arquivo LDBIOS.TXT.

O analisador de inventário usa um método de análise para localizar informações sobre o BIOS. Isso permite pesquisar informações em uma ou mais linhas distantes de uma seqüência de texto especificada. Tal pesquisa permitiria localizar combinações aleatórias de letras e números atribuídas ao hardware do computador.

Seqüências de caracteres no LDBIOS.TXT

Se você executar o analisador de inventário com o parâmetro de linha de comando /do16 durante uma análise de inventário, as seqüências de texto disponíveis no BIOS serão exportadas para um arquivo de texto denominado LDBIOS.TXT. LDBIOS.TXT armazena todas as seqüências que são criadas pelo analisador. Se desejar armazenar essas informações no banco de dados, poderá armazená-las como um arquivo de configuração usando o parâmetro CFGFILES em Ldappl3.ini.

Exemplo de entradas do BIOS no arquivo LdAppl3.Template

A seguir está um exemplo da seção [BIOS Info] no arquivo Ldappl3.Template:

```
[BIOS Info]
StringLength=4
Key = BIOS - Manufacturer
Parameters = AllValues,FirstInstance
Value = AMI|American Megatrends::AMI::BIOS - AMI
Value = Copyright.*Dell::Dell::BIOS - Dell
[BIOS - AMI]
Key = % - Version
Parameters = FirstValue,FirstInstance
Value = BIOS Version \(.*\)::\1
Key = % - Copyright Notice
Parameters = AllValues,AllInstances
Value = ©.*\(AMI|American Megatrends\)
[BIOS - Dell]
Key = % - Version
Parameters = FirstValue,FirstInstance
Value = BIOS Version \(A.+\)::\1
Value = BIOS Version: \(A.+\)::\1
Key = % - Copyright Notice
Parameters = AllValues,AllInstances
Value = ©.*Dell|[Cc]opyright.*Dell
```

Compreensão das entradas do BIOS

As entradas na seção [BIOS Info] consistem em:

- **[Nome da seção]** Identifica um novo componente no banco de dados núcleo.
- **StringLength=** Especifica o tamanho mínimo das sequências da pesquisa.
- **Chave=** Identifica a classe e o nome de atributo das informações retornadas de uma pesquisa no arquivo LDBIOS.TXT.
- **Parâmetros=** Especifica os critérios de pesquisa que instruem o analisador sobre onde e como pesquisar por valores associados a uma chave específica.
- **Valor=** Especifica o valor da pesquisa no BIOS. Um valor contém três seções principais, cada uma separada por dois dois-pontos (::). As sequências identificadas na entrada do valor diferenciam maiúsculas e minúsculas. Todos os caracteres no valor, até mesmo espaços, são incluídos na pesquisa a menos que eles sejam um operador.

Solução de problemas e tarefas extras do inventário

Este tópico fornece informações adicionais sobre a análise de inventário, bem como algumas dicas para solução de problemas. Também inclui as seguintes informações:

- "Agendamento de uma tarefa de análise de inventário" na página 172
- "Análise de dispositivos independentes" na página 172

- "Adição de registros de inventário ao banco de dados núcleo" na página 172
- "Criação de arquivos MIF" na página 173
- "Verificação de dados personalizados em dispositivos da Macintosh" na página 173
- "Solução de problemas do analisador de inventário" na página 176

Agendamento de uma tarefa de análise de inventário

Se o dispositivo estiver executando os agentes Management Suite, você pode agendar um script que dispara uma varredura de inventário nos dispositivos.

Para agendar uma análise de inventário

1. Clique em **Ferramentas > Distribuição > Tarefas agendadas**.
2. Na barra de ferramentas, clique no botão **Agendar análise de inventário** .
3. Configure destinos de tarefa e horário de início na janela **Tarefas agendadas**.

O script do analisador de inventário está localizado no diretório \Arquivos de programas\LANDesk\ManagementSuite\Scripts. O script é um arquivo .ini do Windows que pode ser editado com qualquer editor de texto. Se for necessário alterar as opções ou os parâmetros dentro do script, abra-o e siga as instruções contidas nele.

Análise de dispositivos independentes

Para analisar um dispositivo independente

1. Copie o analisador de inventário correto e um arquivo de descrição do software (geralmente o LdAppl3.ini) em um disquete. (Pode ser que seja necessário copiar também os arquivos elogapi.dll, ygrep32.dll, locv16vc0.dll, inv16.exe, loc32vc0.dll, ltapi.dll, e ldiscn32.exe.)
2. Execute a análise com **/O= parâmetro** especificando o caminho e o nome do arquivo de saída.
3. No prompt da linha de comando, insira um **nome exclusivo** para o dispositivo. Este nome também será exibido no campo Descrição do banco de dados núcleo. Por exemplo:

```
ldiscn32.exe /f /v /o=c:\%computername%.scn
```

4. Copie o arquivo de análise resultante para a pasta ..\ManagementSuite\ldscan do do servidor núcleo para que seja adicionado ao banco de dados.

Para analisar um dispositivo que tenha acesso ao servidor núcleo através da rede.

1. Mapeie uma unidade (N: por exemplo) para o diretório ldlogon do servidor núcleo onde você deseja que a análise seja realizada.
2. Clique em **Iniciar > Executar** e digite o seguinte comando:

```
N:\LDISCN32.EXE /NTT=CORESERVERNAME:5007 /S="CORESERVERNAME"
/I=HTTP://CORESERVERNAME/ldlogon/ldappl3.ldz /V /F /SYNC
```

Adição de registros de inventário ao banco de dados núcleo

É possível adicionar informações de inventário de um dispositivo independente ou de arquivos de inventário separados, executando o analisador de inventário na linha de comando do sistema operacional.

Para adicionar registros de inventário de um arquivo ao banco de dados núcleo:

- Execute o utilitário de análise com os parâmetros /S=, /T= e /NTT.

Criação de arquivos MIF

Se um arquivo MIF precisar armazenar informações de inventário de um dispositivo, é possível criar um executando o analisador apropriado na linha de comando.

Para criar um arquivo MIF unicode, use a opção /MUNI. Para criar um arquivo MIF não-unicode, use a opção /M.

Para criar arquivos MIF:

- Digite isto no aviso do DOS:

```
LDISCN32/MUNI/V
```

Verificação de dados personalizados em dispositivos da Macintosh

Você pode obter dados personalizados de dispositivos que estajam executando o agente LANDesk para o Macintosh e processá-lo no inventário. As informações são salvas em arquivos XML dentro de um diretório específico no dispositivo cliente. Use as informações abaixo para criar arquivos XML de dados personalizados no local correto para serem processador no inventário.

Para se inteirar das informações sobre uma solução alternativa para dados personalizados para Macintosh. Descarregue a publicação técnica sobre os dados personalizados para Macintosh de http://community.landesk.com/support/docs/DOC-1570.

NOTA: A implementação dos dados personalizados com o agente LANDesk para Macintosh não usa formulários de dados personalizações. As tarefas de formulário de dados personalizados não podem ser distribuídas com sucesso para dispositivos que executam o agente LANDesk para Macintosh.

Arquivo XML de dados personalizados

Antes de poder adicionar dados personalizados a uma análise de inventário de um dispositivo executando o agente LANDesk para Macintosh, é necessário criar um arquivos XML de dados personalizadosno formato correto. Esta seção delineia o formato correto para ativar um arquivo XML de dados personalizados para ser processado sem erro.

Regras de arquivo XML de dados personalizados

Arquivos XML usados para armazenar dados personalizados precisam conformar-se às seguintes regras. Os arquivos XML de dados personalizados que não corresponderem a todas as regras não serão processador no inventário.

- Os arquivos XML de dados podem ter qualquer nome, mas precisam terminar com a extensão .xml. Por exemplo:

```
Phone Numbers.xml
```

- A primeira linha em um arquivo XML de dados personalizados precita ser uma declaração XML. Por exemplo:

```
<?xml version="1.0" encoding="UTF-8"?>
```

- Todas as tags iniciais dentro de um arquivos XLM de dados personalizados precisam ter uma tag final correspondente. Por exemplo:

```
<Home>(123) 456-7890</Home>
```

- Todas as tags dentro de um arquivo XLM de dados personalizados não devem ter espaços. Por exemplo:

```
<Phone_Numbers></Phone_Numbers>
```

- Todos os elementos dentro de um XML de dados personalizados que representam uma única linha de informações precisam ser incluídos dentro de um elemento pai. Por exemplo:

```
<Phone_Numbers><Home>(123) 456-7890</Home></Phone_Numbers>
```

- No caso de não haver conteúdo em um elemento de arquivo XML de dados personalizados, o nome do elemento não será mostrado como um item de dados personalizados no inventário. Por exemplo:

```
<Home></Home>
```

- No caso de não haver conteúdo em nenhum dos elementos aninhados dentro de um elemento pai em um arquivo XML de dados personalizados, o nome do elemento pai não será mostrado como um nó sob os dados personalizados no inventário. Por exemplo:

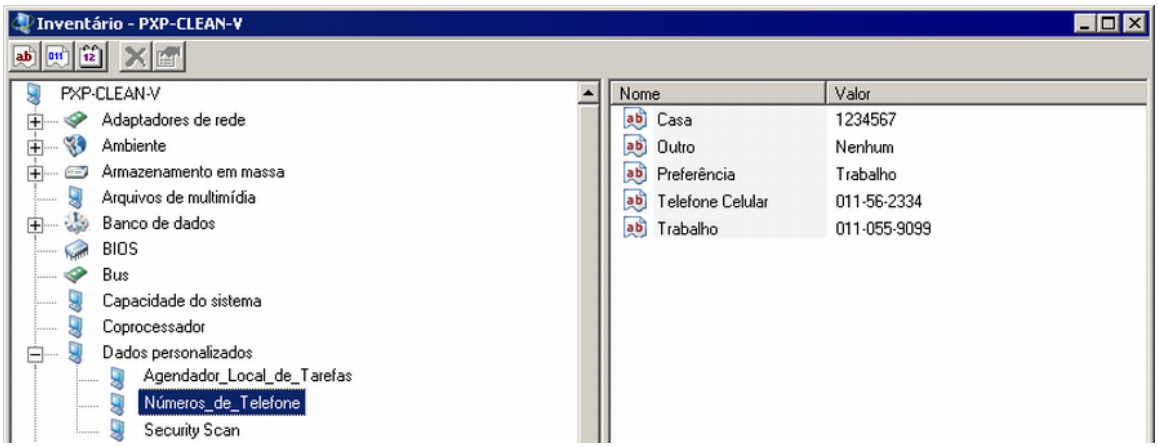
```
<Phone_Numbers><Home></Home><Work></Work></Phone_Numbers>
```

Arquivo XML de dados personalizados de entrada única

Os arquivos XML de dados personalizados podem ser criados para inserir uma única entrada na seção de dados personalizados do inventário. Para fazer isso, as tags de cada elemento em um arquivo XML de dados personalizados precisam ser nomeados com a string que será mostrada no inventário. E então o conjunto de elementos precisa ser aninhado em elementos pais com tags denominadas para representar a string que é para ser mostrada sobr os dados personalizados na tela da árvore no inventário.

Por exemplo, se um arquivo XML de dados personalizados fossem usados para coletar números de telefone, o seguinte formato XLM resultaria no inventário registrado ilustrado abaixo:

```
<?xml version="1.0" encoding="UTF-8"?>
<Phone_Numbers>
<Work>123-456-7890</Work>
<Mobile>(123) 456-7890</Mobile>
<Home>1234567890</Home>
<Other>N/A</Other>
<Preference>Trabalho</Preference>
</Phone_Numbers>
```

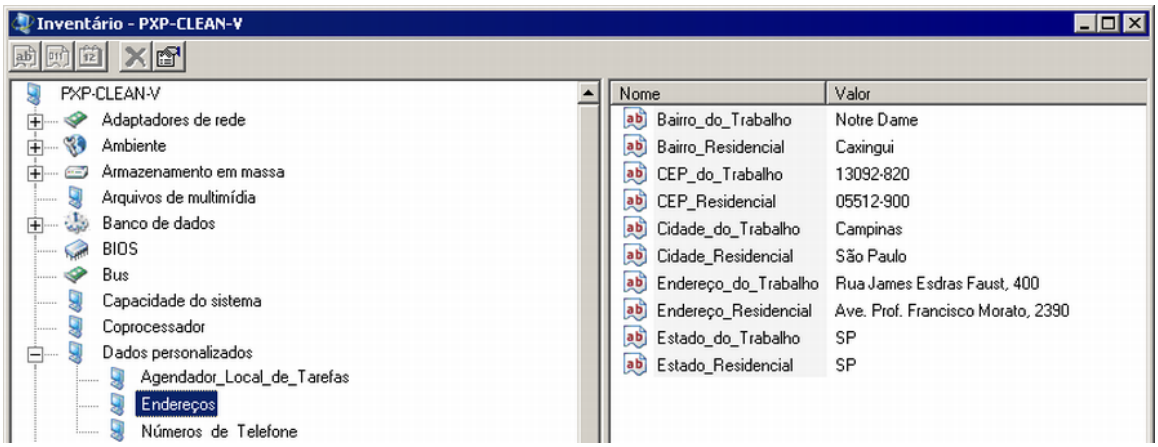


Arquivo XML de dados personalizados de múltipla entrada

Os arquivos XML de dados personalizados podem ser criados para inserir entradas múltiplas na seção de dados personalizados do inventário. Para fazer isso, as tags de cada elemento em um arquivo XML de dados personalizados precisam ser nomeados com a string que será mostrada no inventário. E então cada conjunto de elementos precisa ser aninhado em elementos pais com tags denominadas para representar a string que é para ser mostrada sobr os dados personalizados na tela da árvore no inventário.

Por exemplo, se um arquivo XML de dados personalizados fossem usados para coletar dados dos funcionários, o seguinte formato XLM resultaria no inventário registrado ilustrado abaixo:

```
<?xml version="1.0" encoding="UTF-8"?>
<Phone_Numbers>
<Work>123-456-7890</Work>
<Mobile>(123) 456-7890</Mobile>
<Home>1234567890</Home>
<Other>N/A</Other>
<Preference>Trabalho</Preference>
</Phone_Numbers>
<Addresses>
<Work_Address_1>Rua Tucunaré, 123</Work_Address_1>
<Work_Address_2>Suite 550</Work_Address_2>
<Work_Address_3></Work_Address_3>
<Work_City>São Luis</Work_City>
<Work_State>MA</Work_State>
<Work_ZIP_Code>CEP 463102</Work_ZIP_Code>
<Home_Address_1>Via Elmo, 456</Home_Address_1>
<Home_Address_2></Home_Address_2>
<Home_Address_3></Home_Address_3>
<Home_City>São Luis</Home_City>
<Home_State>MA</Home_State>
<Work_ZIP_Code>CEP 463102</Work_ZIP_Code>
</Addresses>
<Employee_Information>
<Title>Representante de vendas</Title>
<Employee_ID>4562</Employee_ID>
<Manager>Roberto Smith</Manager>
<E-Mail>John.Doe@WidgetsNMore.com</E-Mail>
</Employee_Information>
```



Diretório de dados personalizados

Cada arquivo XML de dados personalizados a ser processado no inventário precisa ser salvo no diretório de dados personalizados, que está localizado em **/Library/Application Support/LANDesk/CustomData** em cada dispositivo que executa o agente LANDesk para Macintosh.

Após um arquivo XML de dados personalizados ser processador no inventário, o arquivos permanece no diretório CustomData. Isto permite análises completas subsequentes (e análises delta com **Forçar análise de software** ativada) para incluir as informações dos arquivos XML de dados personalizados salvos no diretório de dados personalizados.

Inventário

Durante a parte do software de uma análise de inventário, é feita uma verificação do diretório CustomData. Quaisquer arquivos XML no diretório CustomData serão processados para os dados personalizados e incluídos na análise de inventário enviada para o núcleo.

Tipos de análises de inventário

Os arquivos XML de dados personalizados que estão no diretório CustomData são processados durante todas as análises completas e são também processados durante as análises delta que incluem a análise de software.

Registro de inventário

A parte de uma análise de inventário que procura e processa arquivos XML de dados personalizados é registrada em LANDesk.log como **ldscan**:**Análise de dados personalizados.** Se os arquivos XML de dados personalizados no diretório CustomData forem formatados corretamente, não haverá mais entradas no LANDesk.log relacionadas aos dados personalizados. Entretanto, se houver um erro, ele será registrado no LANDesk.log como **ldscan**:**Erro ao abrir ou carregar o arquivo CustomData: filename.xml como XML.**

Um erro durante o processamento de um arquivo XML de dados personalizados não impede outros arquivos desse tipo salvos no diretório de dados personalizados de serem processados. Da mesma forma, os erros de processamento de arquivos XML de dados personalizados não impedirão uma análise de inventário de concluir ou de ser enviada para o núcleo.

Inventário no núcleo

Informações de dados personalizados no inventário, para um dispositivo executando o agente LANDesk para Macintosh, será atualizado quando os arquivos XML de dados personalizados contendo informações forem atualizados e uma análise de inventário que atualiza dados personalizados for executada no cliente.

Esteja alerta para fato de que as informações de dados personalizados removidas dos arquivos XML de dados personalizados não são removidas dos registros do inventários no núcleo. Para remover informações de dados personalizados não desejados de um registro de inventário do núcleo, exclua o registro e envie uma nova análise completa do dispositivo que o registro representava.

Solução de problemas do analisador de inventário

Esta seção descreve problemas comuns do analisador de inventário e como solucioná-los.

O analisador de inventário não responde

- Verifique se as opções /DELL ou /CPQ anteriores não estão inclusas na linha de comando. Essas opções não são mais suportadas.
- Analise um arquivo por meio do parâmetro /O=. Esse procedimento pode indicar um conflito com a placa de rede ou a rede.

As análises de hardware de um dispositivo são executadas corretamente, mas as de software não

- Verifique se o banco de dados núcleo está configurado para executar uma análise de software agora e use o parâmetro /f para forçar uma análise de software.
- Analise um arquivo por meio do parâmetro /O=. Esse procedimento deve listar todo o software no final do arquivo.

- Verifique se o dispositivo não está tentando analisar um arquivo binário no parâmetro CfgFiles do LdAppl3.Template.

A tela de rede fornece dados de inventário apenas para alguns dispositivos

Para exibir informações de dispositivos, verifique se os dispositivos foram analisados no banco de dados núcleo. Os dispositivos que forem exibidos sem informações não terão sido analisados no banco de dados núcleo.

Para exibir os dados de inventário de um dispositivo na tela de rede

1. Configure o dispositivo.
2. Analise o dispositivo no banco de dados núcleo.

Especificação do número de dias que deseja manter as análises de inventário.

Por padrão, o servidor núcleo mantém análises de inventário para dispositivos até você os excluir. Você pode fazer o núcleo excluir análises de inventário para dispositivos se o dispositivo não tiver submetido uma análise para o número de dias que especificar. Isso pode remover dispositivos que não estão mais na sua rede.

Para especificar o número de revisões de arquivo que manterá no banco de dados núcleo

1. Clique em **Configurar > Serviços > Inventário**.
2. Especifique o número de dias que deseja manter as análises de inventário.
3. Clique em **OK**.

Altera a forma como o analisador de inventário coleta informações do BIOS

A partir do Management Suite 8.7 SP3, 8.7 SP3, o analisador de inventário não usa mais o analisador de 16 bits para coletar algumas informações do BIOS. Por padrão, o analisador não relata mais o número de barramento da motherboard, os atributos de dispositivos do barramento da motherboard e o tamanho das unidades de disquete conectadas. Além disso, o analisador de inventário não cria mais um arquivo LDBIOS.TXT oculto com as seqüências de caracteres do BIOS nos dispositivos gerenciados.

Para fazer com que o analisador de inventário relate novamente essas opções e crie o arquivo LDBIOS.TXT, você poderá executar o analisador de inventário com a chave /do16.

Ajuda do inventário

Sobre a janela Inventário

Use a janela **Inventário** para exibir o inventário completo de um dispositivo, incluindo os seguintes componentes:

- **BIOS:** Tipo, data, bytes do ID, fabricante, versão da ROM, versão do SMBIOS e modelo do sistema para o BIOS. O BIOS reside permanentemente na ROM (Memória somente leitura) do computador e permite a comunicação da memória, das unidades de disco e do monitor do computador.
  Outras informações da BIOS aparecem na janela Inventário como seqüências de texto da BIOS. Para ver e pesquisar seqüências de texto do BIOS, expanda o objeto **BIOS**, selecione **Seqüências do BIOS**, clique o botão direito no atributo **Dados**, selecione **Propriedades** e, em seguida, clique em **Valores estendidos**. Durante uma varredura de inventário, as seqüências de texto disponíveis do BIOS são exportadas para um arquivo de texto, LDBIOS.TXT. É possível configurar uma consulta no arquivo LDAPPL3.INI que envie uma ou mais das seqüências de texto do BIOS ao console. Para obter

mais informações, consulte "Adição de sequências de texto do BIOS ao banco de dados do núcleo" na página 170 .

- **Barramento:** Tipo de barramento. O barramento conecta o microprocessador, as unidades de disco, a memória e as portas de entrada/saída. Os tipos de barramento podem ser ISA, EISA, Barramento local VESA, PCI e USB.
- **Co-processador:** Tipo de co-processador, se houver. O co-processador é diferente do microprocessador principal, embora ele possa residir na mesma placa-mãe ou ainda no mesmo chip. O co-processador matemático avalia as operações de ponto flutuante para o microprocessador principal.
- **Dados personalizados:** Quais quer dados personalizados habilitados para o analisador de inventário.
- **Banco de dados:** Informações sobre o driver e a versão do banco de dados.
- **Ambiente:** Locais de arquivos, caminho de comandos, prompt do sistema e outras variáveis para o ambiente Windows.
- **Funcionamento:** Funcionamento do dispositivo conforme determinado pelo agente LANDesk.
- **Teclado:** Tipo de teclado conectado ao dispositivo. Atualmente, o tipo mais comum de teclado é o teclado avançado IBM. A página de código é a linguagem que o teclado usa.
- **LANDesk Management:** Informações sobre os agentes, o gerenciador de clientes e o AMS (Alert Management System). Além disso, contém informações sobre a varredura de inventário e os arquivos de inicialização.
- **Usuários e grupos locais:** O grupos de usuários e a participação em grupo locais do Windows.
- **Armazenamento em massa:** Dispositivos de armazenamento no computador, incluindo unidades de disquete, discos rígidos, unidades lógica e de fita e CD-ROM. Os objetos Disco rígido e Unidade de disquete incluem os atributos de cabeçalho, número, setor e armazenamento total.
- **Memória:** Atributos de memória virtual, física e arquivo de paginação. Cada um desses objetos Memória inclui atributos de byte. O primeiro byte corresponde à quantidade de memória disponível. O segundo byte corresponde à memória total.
- **Modems:** Informações do modem, inclusive: fabricante, modelo, número e porta.
- **Placa-mãe:** Informações da Placa-mãe, inclusive a velocidade de bus e informações sobre slots.
- **Mouse:** Tipo de mouse conectado ao dispositivo. Os valores de tipo de mouse incluem PS/2, serial e infravermelho.
- **Arquivos de multimídia** Número de arquivos com extensões comuns de arquivos multimídia (.jpg, .mp3 etc) e quanto de espaço eles ocupam.
- **Rede:** Informações sobre adaptador de rede, endereço NIC e endereço do nó do adaptador. O objeto Rede inclui informações de cada protocolo.
- **Adaptadores de rede:** Atributos para cada adaptador de rede instalado no dispositivo.
- **SO:** Sistema operacional, drivers, serviços e portas. Esses objetos e seus atributos variam de acordo com as configurações dos drivers e serviços carregados.
- **Portas:** Objetos para cada uma das portas de saída do computador (serial e paralela). Cada porta de saída contém atributos de endereço e nome. O atributo de endereço contém o endereço de hardware da porta.
- **Gerenciamento de energia:** Configurações de gerenciamento de energia no dispositivo.
- **Impressoras:** Objetos para cada impressora conectada ao computador, diretamente ou por uma rede. Os objetos Impressora contêm atributos de driver, nome, número e porta. O atributo de porta contém a fila da rede ou a porta à qual a impressora está conectada.

- **Processador:** Atributos da CPU do dispositivo. Detecta os processadores Intel, Motorola 680x0 e PowerPC.
- **Recursos:** Objetos para cada recurso de hardware do computador. Cada objeto Recurso de hardware contém atributos que descrevem o tipo de recurso e quaisquer portas e interrupções sendo usadas.
- **Segurança:** Software e versão de antivírus.
- **Software:** Objetos para cada aplicativo de software instalado no disco rígido do cliente. Cada objeto Programa de software lista os atributos que geralmente contêm o nome, o local e o número da versão do software.
- **Sistema:** Informações sobre a placa-mãe e o chassi.
- **Capacidade do sistema:** Diversas tecnologias de sistemas, como ASIC ou software de máquina virtual.
- **Tecnologias ThinkVantage:** Informações sobre o software das tecnologias Lenovo ThinkVantage.
- **Vídeo:** Objetos para cada adaptador de vídeo no dispositivo. O objeto Adaptador de vídeo geralmente contém atributos que descrevem a resolução e o número de núcleos suportados.

Sobre a caixa de diálogo Propriedades do atributo de inventário

Use essa caixa de diálogo para exibir as propriedades de um atributo. A guia **Características** pode mostrar as seguintes informações. Conforme o atributo e se for adicionar, editar ou ver um atributo, nem todos os campos aparecerão.

- **Nome:** O nome do atributo do banco de dados núcleo cujas propriedades você está visualizando.
- **Valor:** O valor atribuído a este atributo de inventário.
- **Definido pelo usuário:** Indica se o atributo selecionado foi definido ou não pelo usuário. Não é possível alterar essa opção.
- **Especificador de formato (valores de número inteiro apenas):** Notação usada para exibir o valor em formato apropriado. Por exemplo, %d MB exibe o valor de atributo sem valores decimais; %.1f MB exibe o valor de atributo no primeiro ponto decimal flutuante em unidades de MB. Se nenhum valor de fator for digitado, esse especificador de formato deverá descrever os valores de número inteiro (%d). Se um valor do fator for digitado, esse especificador de formato deverá descrever os valores de ponto flutuante (%f).
- **Fator (valores de número inteiro apenas):** Valor de número inteiro usado para dividir o atributo em unidades. Se você alterar o valor do fator, será necessário digitar o código apropriado no campo do especificador de formato. Por exemplo, para exibir o número de megabytes se o atributo for gravado em quilobytes, digite o valor 1000.
- **Valor formatado:** Exemplo de texto demonstrando o formato e o fator especificado.

Sobre a caixa de diálogo Configurações de alterações no inventário

Use essa caixa de diálogo para selecionar quais atributos de inventário são registrados quando ocorrerem alterações em dispositivos individuais e determinar onde essas alterações são registradas.

- **Inventário atual:** Relaciona todos os objetos armazenados no banco de dados núcleo. Clique em um objeto para mostrar seus atributos na lista **Evento de log em**. Expanda um grupo de objetos para ver os objetos Dados que ele contém.

- **Evento de log em:** Relaciona os atributos do objeto Inventário selecionados na lista **Inventário atual**.
  Para definir onde as alterações no inventário serão registradas, selecione um atributo e uma ou mais opções. Selecione a opção **Inventário** para registrar as alterações na caixa de diálogo do dispositivo **Histórico de alterações no inventário**. Selecione a opção **Log do NT** para registrar as alterações no log de eventos do Windows NT. Selecione a opção **AMS** para enviar as alterações como um alerta via o AMS (configure os alertas AMS com a ferramenta Configurações de alertas).
- **Gravidade de log/alerta:** Relaciona as opções de prioridade do alerta. Esse recurso estará esmaecido até que um atributo seja realmente selecionado. Você pode selecionar o nível de gravidade Nenhum, Informações, Aviso ou Crítico.

Sobre a caixa de diálogo Histórico de alterações no inventário

Use essa caixa de diálogo para exibir as alterações no inventário de um dispositivo. Você também pode imprimir e exportar o histórico de alterações no inventário nessa caixa de diálogo.

- **Nome do dispositivo:** Exibe o nome dos dispositivos selecionados na tela de rede do console para os quais são solicitados os dados de alterações no inventário.
- **Componente:** Identifica o componente do sistema que foi alterado. (Somente os componentes selecionados na caixa de diálogo **Configurações de mudanças no inventário** são exibidos aqui.)
- **Atributo:** Identifica o atributo de componente específico sendo registrado.
- **Hora:** Indica quando a alteração ocorreu.
- **Novo valor:** Exibe o novo valor (alterado) do atributo listado.
- **Valor antigo:** Exibe o valor antigo (anterior) do atributo listado.
- **Imprimir:** Abre uma caixa de diálogo Imprimir padrão na qual você pode imprimir o conteúdo do histórico de alterações no inventário.
- **Exportar:** Abre uma caixa de diálogo Salvar como, na qual você escolhe um nome e local para o arquivo CSV exportado que contém o histórico de alterações no inventário.

NOTA: A caixa de diálogo **Histórico de mudanças do inventário** mostra o histórico na ordem cronológica. Não é possível os dados clicando nos cabeçalhos das colunas.

Sobre a caixa de diálogo Criar/editar um formulário de dados personalizados

A LANDesk Security Suite **não oferece suporte à formulários de dados personalizados**

Os formulários de dados personalizados estão indisponíveis apenas na licença do LANDesk Security Suite. É necessário uma licença completa do LANDesk Management Suite a fim de usar o recurso de formulários de dados personalizados.

Use essa caixa de diálogo para criar ou editar um formulário de dados personalizados.

- **Nome do formulário:** Identifica o formulário e aparece na Tela de formulário quando um usuário o preenche.
- **Descrição:** Fornece informações adicionais aos usuários sobre o formulário.
- **Adicionar:** Abre a caixa de diálogo **Adicionar pergunta** na qual você pode criar uma nova pergunta para o formulário.
- **Editar:** Abre a caixa de diálogo **Editar pergunta** na qual você pode editar qualquer uma das opções de pergunta.
- **Excluir:** Remove a pergunta do formulário.

- **Quebra de página:** Controla o layout do formulário adicionando quebras de página às perguntas do grupo nas páginas. Quando há uma quebra de página, os usuários clicam no botão Avançar para continuar com as perguntas na próxima página.

NOTA: O número máximo de perguntas por página é nove.

- **Visualizar:** Abre o formulário para que você possa visualizar como ele se parecerá para os usuários. No modo de visualização, você não deve preencher dados e o que for digitado não será salvo.

Sobre a caixa de diálogo Adicionar/editar pergunta

Use essa caixa de diálogo para criar ou editar as perguntas que aparecem no formulário de dados personalizados. Os formulários consistem em perguntas e em um lugar para os usuários colocarem suas respostas. Em primeiro lugar, identifique a pergunta:

- **Texto da pergunta:** Descrição em uma linha do que está sendo perguntado. Esse texto é exibido ao lado do campo de dados.
- **Nome do inventário:** Nome do campo do banco de dados no banco de dados de núcleo. Se você consultar o banco de dados núcleo quanto a esse item, o ID da etiqueta será sobre o quê você está consultando.
- **Descrição:** Informações adicionais que são exibidas quando os usuários clicam em **Ajuda** (ou pressionam **F1** no campo de dados desta pergunta).

Você também precisa especificar que tipo de campo de dados (controle) mostrar ao lado de cada pergunta e se isso é necessário. Os campos de dados disponíveis são:

- **Editar caixa:** Os usuários digitam suas respostas em uma caixa de texto editável.
- **Caixa combo (editar lista):** Os usuários selecionam um dos itens predefinidos da lista ou digitam um novo item de sua propriedade.
- **Caixa combo (lista fixa):** Os usuários selecionam um dos itens predefinidos da lista.
- **Tornar o controle um campo de preenchimento obrigatório:** Força a resposta do usuário à pergunta. O usuário não pode concluir um formulário ou mover para a próxima página do formulário antes de responder aos campos obrigatórios.

Sobre a caixa de diálogo Adicionar itens

Use essa caixa de diálogo para adicionar itens a uma lista suspensa que o usuário pode escolher ao responder à pergunta em um formulário.

- **Nome do item:** Identifica o item. Esse nome é exibido na lista da pergunta.
- **Lista de itens:** Relaciona todos os itens que são exibidos na lista da pergunta.
- **Inserir:** Coloca o item na Lista de itens.
- **Excluir:** Remove o item da Lista de itens.

Sobre a caixa de diálogo Selecionar vários formulários a serem distribuídos

Use essa caixa de diálogo para criar um grupo de formulários que mostra o nome do grupo e lista os formulários disponíveis que podem fazer parte de um grupo.

- **Nome do grupo:** Identifica o grupo na janela **Formulários de dados personalizados**.
- **Formulários disponíveis:** Relaciona todos os formulários disponíveis que você pode adicionar ao grupo.

- **OK:** Salva o grupo e fecha a caixa de diálogo.
- **Cancelar:** Fecha a caixa de diálogo sem salvar o grupo.

Gerenciador de diretórios/consultas

Consultas de banco de dados

Consultas são pesquisas personalizadas à procura de dispositivos gerenciados. O LANDesk Management Suite oferece um método para pesquisar dispositivos que foram analisados para o banco de dados núcleo através de consultas de banco de dados e, também, um método para procurar dispositivos localizados em outros diretórios através de consultas LDAP. Você vê, cria e organiza consultas de banco de dados com os grupos de Consultas na tela de rede do console.

As consultas ajudam a gerenciar a rede, permitindo que você pesquise e organize os dispositivos de rede existentes no banco de dados núcleo, com base em critérios específicos do sistema ou do usuário.

Por exemplo, você pode criar e executar uma consulta que capture somente dispositivos com uma velocidade do clock do processador menor do que 2 GHz ou com menos de 1.024 MB de RAM ou, então, uma unidade de disco rígido com menos de 20 GB. Crie uma ou mais instruções de consultas que representem essas condições e relacione as instruções umas às outras usando operadores lógicos padrão. Quando as consultas são executadas, é possível imprimir os resultados e acessar e gerenciar os dispositivos correspondentes.

Grupos de consulta

As consultas podem ser organizadas em grupos na tela de rede. Crie novas consultas (e novos grupos de consultas) clicando com o botão direito do mouse no grupo **Minhas consultas** e selecionando **Nova consulta** ou **Novo grupo**, respectivamente.

Um administrador Management Suite (usuário com direitos de administrador Management Suite) pode visualizar o conteúdo de todos os grupos de consulta, inclusive: **Minhas consultas, Consultas públicas e Todas as consultas**

Outros usuários do Management Suite fazem logon no console, eles podem ver as consultas nos grupos **Minhas consultas**, **Consultas públicas** e **Todas as consultas**, com base no escopo de seu dispositivo.

Ao mudar uma consulta para um grupo (clicando com o botão direito do mouse e selecionando **Adicionar a novo grupo** ou **Adicionar a grupo já existente**) ou arrastando e soltando a consulta, na realidade, você está criando uma cópia da consulta. Você pode remover a cópia em qualquer grupo de consultas sem que a cópia principal da consulta (no grupo **Todas as consultas**) seja afetada. Se quiser excluir a cópia principal, poderá fazê-lo no grupo **Todas as consultas**.

Criar uma consulta de banco de dados

Use o diálogo **Nova consulta** para criar uma consulta selecionando entre atributos, operadores relacionais e valores de atributos. Compile uma instrução de consulta escolhendo um atributo de inventário e relacionando-o a um valor aceitável. Relacione logicamente as instruções de consultas umas às outras para garantir que sejam avaliadas como um grupo, antes de relacioná-las a outras instruções ou a outros grupos.

Para criar uma consulta ao banco de dados

1. Na tela de rede do console, clique com o botão direito no grupo **Minhas consultas** (ou **Consultas públicas**, se você tiver direito de gerenciamento de consulta pública) e em **Nova consulta**.
2. Digite um nome exclusivo para a consulta.

3. Selecione um componente naa lista de atributos de inventário.
4. Selecione um operador relacional.
5. Na lista de valores, selecione um valor. Você pode editar um valor.
6. Clique em **Inserir** para adicionar a instrução à lista de consultas.
7. Para consultar mais de um componente, clique em **operador lógico (AND, OR)** e repita as etapas de 2 a 5.
8. (Opcional) Para agrupar instruções de consultas de modo que elas sejam avaliadas como um grupo, selecione duas ou mais **instruções de consultas** e clique em **Agrupar**( ).
9. Quando terminar de adicionar instruções, clique em **Salvar**.

Criar uma consulta de banco de dados

Para executar uma consulta

1. Na tela de rede, expanda os grupos de consultas para localizar a consulta a ser executada.
2. Clique duas vezes na consulta. Ou clique com o botão direito do mouse e selecione **Executar**.
3. Os resultados (dispositivos correspondentes) são exibidos no painel direito da tela de rede.

Importar e exportar consultas

Você pode usar Importar e Exportar para transferir consultas de um banco de dados núcleo para outro. Você pode importar:

- Consultas exportadas das versões 8 e 9 do Management Suite
- Consultas .XML exportadas do console da Web

Para importar uma consulta

1. Clique com o botão direito do mouse no grupo de consultas em que você deseja colocar a consulta importada.
2. No menu de atalhos, selecione **Importar**.
3. Navegue até a consulta a ser importada e selecione-a.
4. Clique em **Abrir** para adicionar a consulta ao grupo de consultas selecionado na tela de rede.

Para exportar uma consulta

1. Clique com o botão direito do mouse na consulta a ser exportada.
2. No menu de atalhos, selecione **Exportar**.
3. Navegue até o local em que deseja salvar a consulta (como um arquivo .ldms).
4. Digite um nome para a consulta.
5. Clique em **Salvar** para exportar a consulta.

Consultas LDAP

Além de consultar o banco de dados núcleo, o Management Suite também oferece a ferramenta gerenciador de diretórios, que permite que você localize, acesse e gerencie os dispositivos em outros diretórios através do LDAP (Lightweight Directory Access Protocol).

Você pode consultar dispositivos com base em atributos específicos, como tipo de processador ou SO. Também é possível executar uma consulta com base em atributos específicos do usuário, como ID ou departamento do funcionário.

Para informações sobre a criação e execução de consultas de banco de dados dos grupos Consultas na tela de rede, consulte "Gerenciador de diretórios/consultas" na página 183.

Configurar diretórios LDAP

Use a ferramenta gerenciador de diretórios para gerenciar os diretórios LDAP que você usa com o LANDesk Management Suite. O servidor LDAP, o nome de usuário e senha que você digite são salvos e usados quando você procura ou executa consultas no diretório. Se você mudar a senha do usuário configurado no diretório LDAP, você deve também mudar a senha nesta ferramenta.

NOTA: A conta que você configurar no gerenciador de diretório deve poder ler os usuários, computadores e grupos que você usa para gerenciar com LDMS.

Para configurar um novo diretório

1. Clique em **Configurar > Gerenciar diretórios**.
2. Clique em **Adicionar**.
3. Digite o nome DNS do servidor de diretórios no campo **LDAP://**
4. Digite o **Nome do usuário** e a **Senha**.

NOTA: Se estiver usando Active Directory, digite o nome como <nome-de-domínio>\<nome-de-usuário-nt> Se estiver usando outro serviço de diretório, digite o nome distinto do usuário

5. Clique em **OK** para salvar as informações. A informação que você digitar é verificada no diretório antes da caixa de diálogo fechar

Para modificar uma configuração de diretório existente

1. Clique em **Configurar > Gerenciar diretórios**.
2. Clique no diretório que desejar.
3. Clique em **Editar**.
4. Mude o servidor, nome de usuário e senha como desejado
5. Clique em **OK** para salvar as informações. A informação que você digitar é verificada no diretório antes da caixa de diálogo fechar

Para excluir uma configuração de diretório existente

1. Clique em **Configurar > Gerenciar diretórios**.
2. Clique no diretório que desejar.
3. Clique em **Excluir**.

NOTA: Todas as consultas LDAP que usam este diretório serão excluídas quando o diretório for removido.

Criar uma consulta ao diretório LDAP

A tarefa de criar e salvar uma consulta em um diretório é dividida em dois procedimentos:

Para selecionar um objeto no diretório LDAP e iniciar uma nova consulta

1. Clique em **Ferramentas > Distribuição > Gerenciador de diretórios**.
2. Acesse o painel de diretórios do **Gerenciador de diretórios** e selecione um objeto no diretório LDAP. Você criará uma consulta LDAP que retorna resultados desse ponto na árvore de diretórios para baixo.
3. No Gerenciador de diretórios, clique no botão **Nova consulta** da barra de ferramentas. Observe que esse ícone será exibido somente quando você selecionar a organização raiz (o) da árvore de diretórios (o=minha empresa) ou uma unidade organizacional (ou=engenharia) na organização raiz. Caso contrário, ele ficará esmaecido.
4. A caixa de diálogo **Consulta LDAP básica** é exibida.

Para criar, testar e salvar a consulta

1. Na caixa de diálogo **Consulta LDAP básica**, clique em um atributo que será um critério para a consulta na lista de atributos de diretório (exemplo = departamento).
2. Clique em um operador de comparação para a consulta (=,<=, >=).
3. Digite um valor para o atributo (exemplo: departamento = engenharia).
4. Para criar uma consulta complexa que combine vários atributos, selecione um operador de combinação (AND ou OR) e repita as etapas de 1 a 3 quantas vezes desejar.
5. Quando terminar de criar a consulta, clique em **Inserir**.
6. Para testar a consulta completa, clique em **Testar consulta**.
7. Para salvar a consulta, clique em **Salvar**. A consulta salva será exibida por nome em **Consultas salvas**, no painel de diretórios do Gerenciador de diretórios.

Sobre a janela do Gerenciador de diretórios

Use o Gerenciador de diretórios para executar as seguintes tarefas:

- **Gerenciar diretório:** Abre a caixa de diálogo **Propriedades do diretório**, onde você pode identificar e fazer logon em um diretório LDAP.
- **Remover diretório:** Remove o diretório selecionado do painel de visualização e interrompe seu gerenciamento.
- **Atualizar modo de exibição:** Recarrega a lista de diretórios gerenciados e usuários direcionados.
- Iniciar a Visualização da organização:
- **Nova consulta:** Abre a caixa de diálogo **Consulta LDAP**, onde você pode criar e salvar uma consulta LDAP.
- **Excluir consulta:** Exclui a consulta selecionada.
- **Execução da consulta:** Gera os resultados da consulta selecionada.
- **Propriedades do objeto:** Mostra as propriedades do objeto selecionado.

Com o uso do gerenciador de diretórios, é possível arrastar grupos LDAP e salvar consultas LDAP nas tarefas agendadas, tornando-as alvos de tarefas.

A janela do gerenciador de diretórios consiste de dois painéis: um painel de diretórios à esquerda e um painel de visualização à direita.

Painel de diretórios

O painel de diretórios exibe todos os diretórios e usuários registrados. Como um administrador, você pode especificar o nome de um diretório registrado e ver uma lista de consultas associadas ao diretório. Você pode criar e, em seguida, salvar novas consultas em um diretório registrado clicando com o botão direito do mouse ou usando menus suspensos. Depois de criar uma consulta, você pode arrastar e soltá-la na janela **Tarefas agendadas** que a tarefa seja aplicada aos usuários que correspondam à consulta.

Painel de visualização

Quando você seleciona uma consulta salva no painel de diretórios do Gerenciador de diretórios, à esquerda da caixa de diálogo, as diretivas e tarefas direcionadas a essa consulta são exibidas no painel de visualização, à direita. Da mesma forma, quando um usuário LDAP individual é selecionado no painel de diretórios, as diretivas e tarefas direcionadas a esse usuário são exibidas no painel de visualização.

Sobre o LDAP (Lightweight Directory Access Protocol - Protocolo de acesso a diretório leve)

LDAP é um protocolo de padrão da indústria para acessar e visualizar informações sobre usuários e dispositivos. O LDAP permite que você organize e armazene essas informações em um diretório. Um diretório LDAP é dinâmico, pois pode ser atualizado conforme a necessidade e é distribuído, protegendo-o de um único ponto de falha. Os diretórios LDAP comuns incluem Novell Directory Services (NDS) e Microsoft Active Directory Services (ADS).

Os exemplos a seguir mostram consultas LDAP que podem ser usadas para pesquisar o diretório:

- Obter todas as entradas: (objectClass=*)
- Obter entradas contendo 'bob' em qualquer lugar do nome comum: (cn=*bob*)
- Obter entradas com um nome comum maior ou igual a 'bob': (cn>='bob')
- Obter todos os usuários com um atributo de e-mail: (&(objectClass=user)(email=*))
- Obter todas as entradas de usuários com um atributo de e-mail e um sobrenome igual a 'smith': (& (sn=smith)(objectClass=user)(email=*))
- Obter todas as entradas com um nome comum que comece com 'andy', 'steve' ou 'margaret': (& (objectClass=User)(| (cn=andy*)(cn=steve*)(cn=margaret*)))
- Obter todas as entradas sem um atributo de e-mail: (!(email=*))

A definição formal do filtro de pesquisa é a seguinte (em RFC 1960):

- <filter> ::= '(' <filtercomp> ')'
- <filtercomp> ::= <and> > <or> > <not> > <item>
- <and> ::= '&' <filterlist>
- <or> ::= '|' <filterlist>
- <not> ::= '!' <filter>
- <filterlist> ::= <filter> > <filter> <filterlist>
- <item> ::= <simple> > <present> > <substring>
- <simple> ::= <attr> <filtertype> <value>

- <filtertype> ::= <equal> > <approx> > <ge> > <le>
- <equal> ::= '='
- <approx> ::= '~='
- <ge> ::= '>='
- <le> ::= '<='
- <present> ::= <attr> '=*'
- <substring> ::= <attr> '=' <initial> <any> <final>
- <initial> ::= NULL > <value>
- <any> ::= '*' <starval>
- <starval> ::= NULL > <value> '*' <starval>
- <final> ::= NULL > <value>

O símbolo <attr> é uma seqüência de caracteres que representa um Tipo de atributo. O símbolo <value> é uma seqüência de caracteres que representa um Valor de atributo cujo formato é definido pelo serviço de diretório subjacente.

Se o <value> precisar conter um dos caracteres * ou (or), use uma barra invertida (\) antes do caractere.

Sobre a caixa de diálogo Consulta LDAP básica

- **Raiz da consulta LDAP:** Selecione um objeto raiz no diretório para essa consulta (LDAP://ldap.xyzcompany.com/ou = America.o = xyzcompany). A consulta que você está criando retornará resultados a partir desse ponto da árvore para baixo.
- **Atributos LDAP:** seleciona atributos para objetos do tipo de usuário.
- **Operador:** seleciona o tipo de operação a ser executada em relação a um objeto LDAP, seus atributos e valores de atributos incluindo igual a (=), menor ou igual a (<=) e maior ou igual a (>=).
- **Valor:** especifica o valor atribuído ao atributo de um objeto LDAP.
- **AND/OR/NOT:** operadores booleanos que podem ser selecionados para suas condições de consulta.
- **Testar consulta:** executa um teste da consulta criada.
- **Salvar:** salva a consulta criada por nome.
- **Avançada:** cria uma consulta usando os elementos de uma consulta LDAP básica, mas de forma livre.
- **Inserir:** insere uma linha de critérios da consulta.
- **Excluir:** exclui uma linha de critérios selecionada.
- **Limpar tudo:** Limpe todas as linhas de critérios da consulta.

Sobre a caixa de diálogo Consulta LDAP avançada

Na caixa de diálogo **Consulta LDAP básica**, clique em **Avançada** para abrir a caixa de diálogo **Consulta LDAP avançada**, que exibe o seguinte:

- **Raiz da consulta LDAP:** Permite a seleção de um objeto raiz no diretório para esta consulta. A consulta que você está criando retornará resultados a partir desse ponto da árvore para baixo.
- **Consulta LDAP:** Permite criar uma consulta usando os elementos de uma consulta LDAP básica, mas de forma livre.

- **Exemplos:** Exibe exemplos de consultas que você pode usar como guia ao criar sua própria consulta de forma livre.
- **Testar consulta:** Permite executar um teste da consulta criada.

A caixa de diálogo **Consulta LDAP avançada** é exibida quando você opta por editar uma consulta que já tenha sido criada. Além disso, se você selecionar um grupo LDAP no gerenciador de diretórios e optar por criar uma consulta a partir desse ponto, a caixa de diálogo **Consulta LDAP avançada** será exibida com uma consulta padrão que exibe os usuários que fazem parte desse grupo. Você não pode alterar a sintaxe dessa consulta padrão; pode apenas salvar a consulta.

Sobre a caixa de diálogo da fonte do Active Directory dialog box:

Na barra de ferramentas do gerenciador de diretórios, clique em **Gerenciador de diretórios** para abrir a caixa de diálogo **Origem do Active Directory**. Essa caixa de diálogo permite iniciar o gerenciamento de um novo diretório ou exibir propriedades de um diretório gerenciado no momento. Exibe também o URL do servidor LDAP e as informações de autenticação necessárias para estabelecer uma conexão com o diretório LDAP:

- **Caminho do diretório:** Permite especificar o diretório LDAP a ser gerenciado. Um exemplo de um diretório LDAP e a sintaxe correta é ldap.<nome_da_empresa>.com. Por exemplo, você digitaria ldap.xyzcompany.com.
- **Autenticação:** Permite o início da sessão como o seguinte usuário (ou seja, você especifica um caminho, um nome e a senha do usuário).

Sobre a caixa de diálogo Salvar consulta LDAP básica

Na caixa de diálogo **Consulta LDAP básica**, clique em **Salvar** para abrir a caixa de diálogo **Salvar consulta LDAP**, que exibe o seguinte:

- **Escolher um nome para essa consulta:** Permite escolher um nome para a consulta criada.
- **Consultar detalhes da raiz LDAP:** Permite criar uma consulta usando os elementos de uma consulta LDAP básica, mas de forma livre.
- **Consultar detalhes da consulta LDAP:** Exibe exemplos de consultas que você pode usar como guia ao criar sua própria consulta de forma livre.
- **Salvar:** Permite salvar a consulta criada por nome. A consulta é salva no item **Consultas salvas** na entrada Diretório LDAP do painel de diretórios do gerenciador de diretórios.

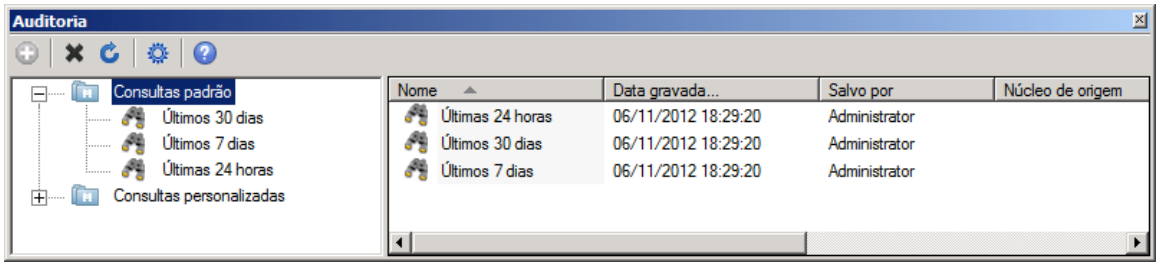
Auditoria

Bem vindo a auditoria

A ferramenta de auditoria audita a atividade do usuário do console e armazena informações de auditoria no banco de dados do núcleo e opcionalmente no log de eventos do Windows.

A ferramenta de auditoria não é habilitada ou visível por padrão. Antes que você possa usar auditoria, você deverá dar ao usuário o direito de configurar a auditoria e depois configurar quais atividades você deseja que sejam auditadas.

Se você ainda não configurou a auditoria, somente as mudanças de configuração de auditoria são auditadas, assim como dar ou remover direitos.



Para mais informações, veja esses tópicos adicionais:

- "Configurando auditoria" na página 190
- "Enviando eventos de auditoria para o Visualizador de eventos do Windows" na página 193
- "Exibição de eventos de auditoria" na página 194
- "Criando filtros para consultas de evento de auditoria" na página 195

Configurando auditoria

A ferramenta de auditoria não é habilitada ou visível por padrão. Antes que você veja a ferramenta de auditoria ou faça mudanças de configuração de auditoria, um administrador deve dar a função de auditor ou de configurador de auditoria.

Existem duas formas de auditoria:

- **Configuração de auditoria:** Usuários com essa função pode configurar o que será auditado. Essa função também inclui os direitos da função de auditor, para que os usuários também possam visualizar a ferramente de auditoria e visualizar os dados de auditoria.
- **Auditor:** Usuários com essa função podem visualizar os dados de auditoria e criar pesquisas personalizadas de auditoria.

Existem três principais passos para configurar a auditoria:

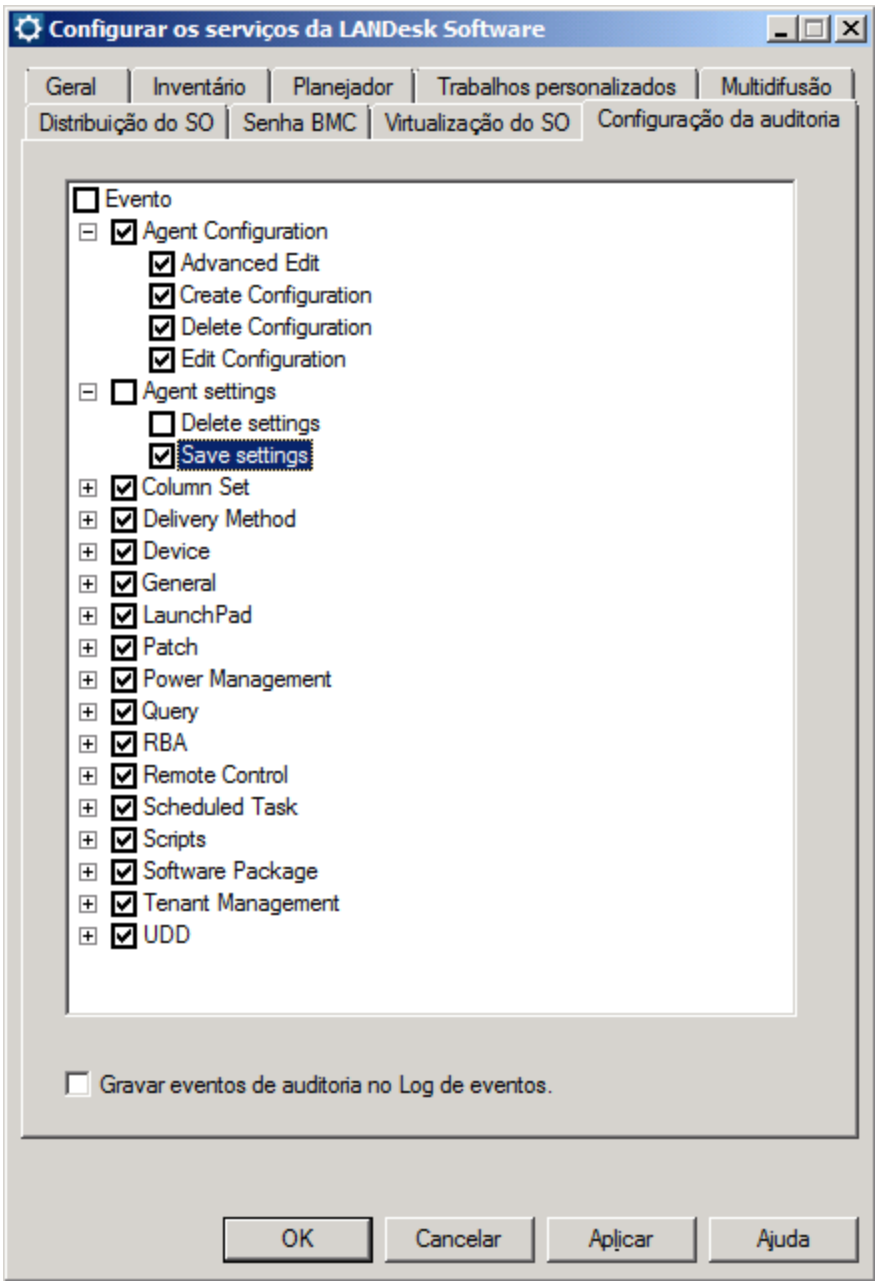
1. Dar ao usuário a função de configurar a auditoria
2. Configurar o que for auditado
3. Atribuir a função de editor aos usuários adicionais se necessário.

Dar a um usuário a função de configuração de auditoria

1. Clique em **Ferramentas > Administração > Gerenciamento de usuários**.
2. No circuito **Funções,** dê um clique duplo em **Configurações de auditoria.**
3. Na página de **Usuários e grupos,** selecione usuários que terão a função de configurar auditoria.
4. Clique em **OK**.
5. Certifique-se que o usuário do console a quem você deu a função de auditoria reinicie seu console para que possa ver a ferramenta de auditoria. As permissões de funções do usuário são carregados assim que o console é iniciado, isso pode causar o reinício do console.

Para configurar o que você quer auditar

1. Clique em **Ferramentas > Serviços de configuração.**
2. Nos **Serviços de configuração de software da LANDesk,** clique na aba **Configuração de auditoria.** Se está guia não estiver visível, certifique-se de que você tem a função de configuração de auditoria e que você reiniciou o console depois de receber essa função.



3. Selecione as características ou sub-características que você quer auditar.
4. Clique em **OK**.
5. Clique em **Ferramentas > Administração > Auditoria** para visualizar os dados a serem auditados.

NOTA: Isso pode levar até dois minutos para que as mudanças da função Gravar eventos de auditoria para o registro de eventos tenha efeito. Você pode reiniciar o console se não quiser esperar.

Para atribuir as funções de auditor para outros usuários

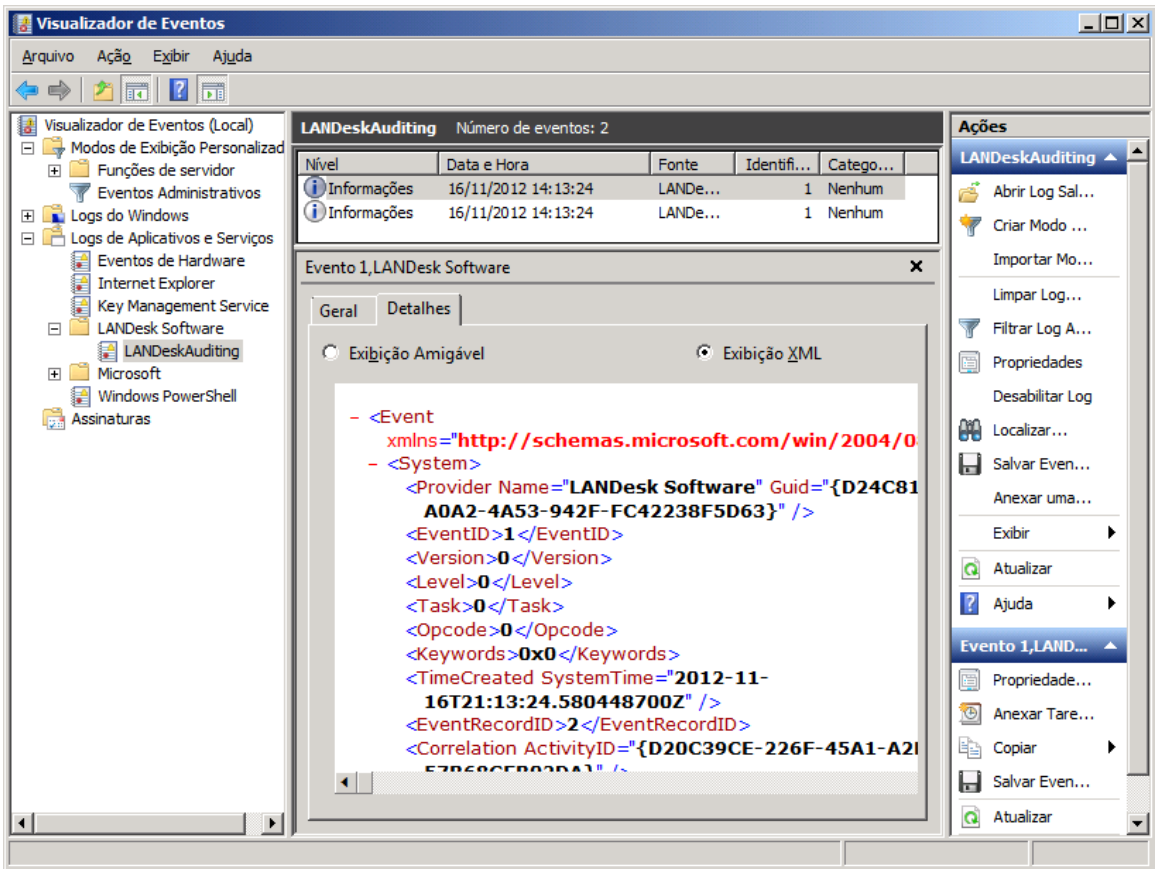
1. Clique em **Ferramentas > Administração > Gerenciamento de usuários**.
2. No circuito **Funções,** dê um clique duplo em **Auditor**.
3. N página de **Usuários e grupos,** selecione os usuários que terão a função de auditor.
4. Clique em **OK**.
5. Faça com que esses usuários reiniciem seus consoles para que a ferramenta de auditoria seja exibida.

Enviando eventos de auditoria para o Visualizador de eventos do Windows

O LANDesk Management Suite armazena eventos de auditoria no núcleo do banco de dados. Você também pode enviar eventos de auditoria para o aplicativo Visualizador de eventos do Windows. Todos os usuários com direitos para exibir o Visualizador de eventos poderá ver as entradas do log da auditoria. Se for um problema de segurança em seu ambiente, considere proteger as entradas do log da auditoria do Visualizador de eventos ou não habilite esta opção.

O Management Suite registra os eventos de auditoria neste caminho do Visualizador de eventos do Windows:

- Logs de serviços e aplicativos > LANDesk Software > LANDeskAuditing



Para enviar eventos de auditoria para o Visualizador de eventos do Windows

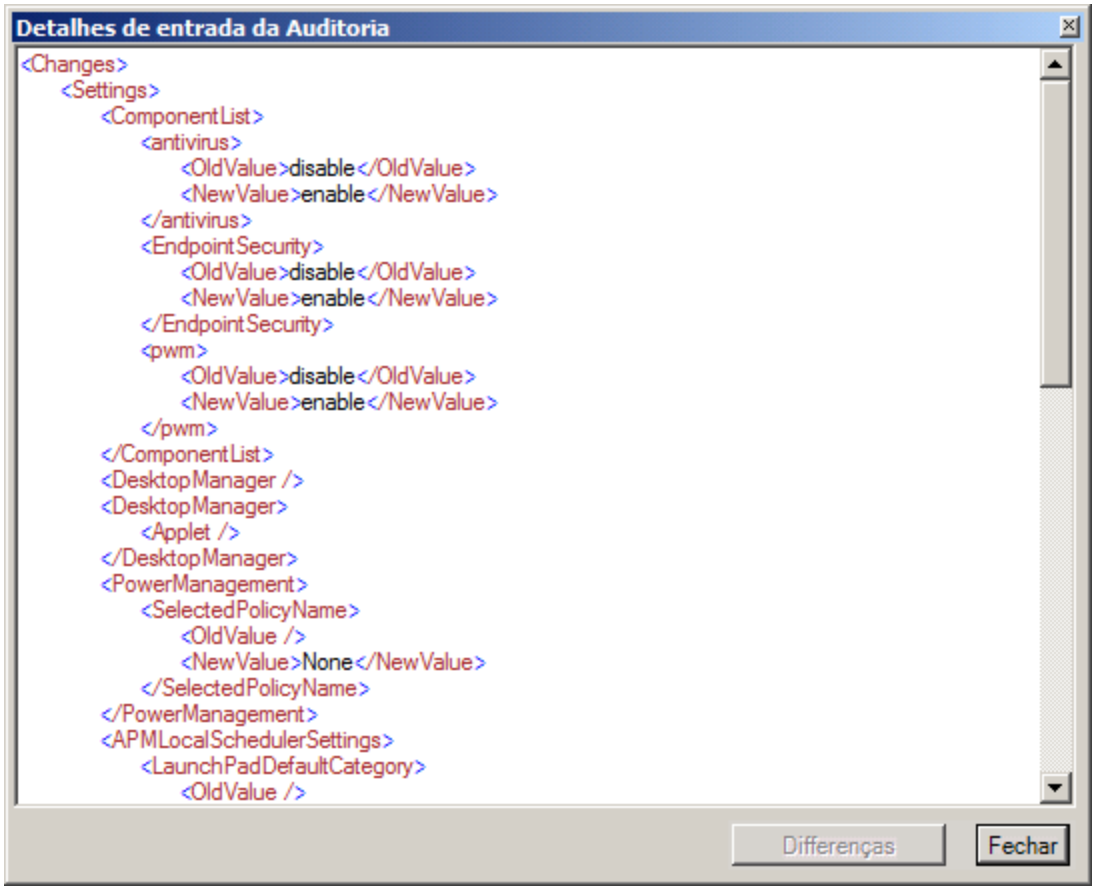
1. Clique em **Ferramentas > Serviços de configuração.**
2. Na caixa de diálogo de **Configurar os serviços da LANDesk Software,** clique na guia **Configurações de auditoria** e selecione **Gravar eventos de auditoria no Log de eventos.** Se está guia não estiver visível, certifique-se de que você tem a função de configuração de auditoria e que você reiniciou o console depois de receber essa função. Ao habilitar esta opção, uma janela de DOS abrirá e fechará rapidamente. Isso é normal.
3. Clique em **OK**.

Habilitando o registro do Visualizador de eventos afetará somente os eventos que acontecerem depois que você habilitar.

NOTA: Isso pode levar até dois minutos para que as mudanças da função Gravar eventos de auditoria para o registro de eventos tenha efeito. Você pode reiniciar o console se não quiser esperar.

Exibição de eventos de auditoria

Eventos de auditoria são armazenados no núcleo do banco de dados em formato XML. Quando você clica duas vezes em um evento de auditoria para visualizá-lo, você verá os itens de XML registrados associados ao evento. Os itens registrados dependem do evento de auditoria.



As consultas padrão de eventos de auditoria cobrem os períodos de tempo a seguir:

- Últimos 30 dias
- Últimos 7 dias
- Último dia

Para visualizar os eventos de auditoria com as consultas padrão

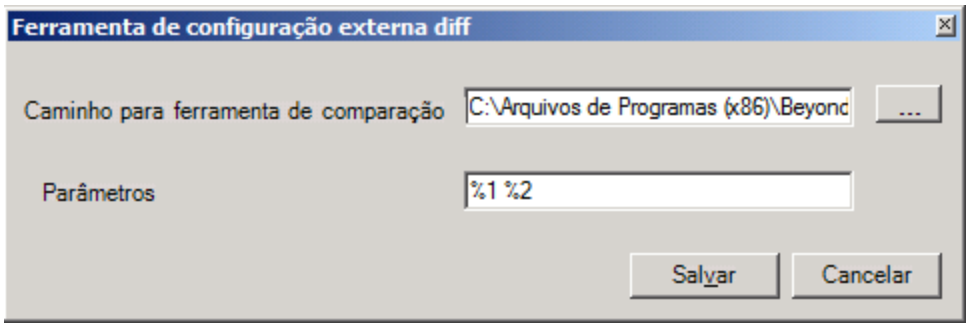
1. Clique em **Ferramentas > Administração > Auditoria**.
2. Na árvore de consultas padrão, clique na consulta desejada.

Você também pode criar filtros personalizados para as consultas da auditoria. Para obter mais informações, veja "Criando filtros para consultas de evento de auditoria" na página 195.

Identificando o que mudou em um evento de auditoria

Alguns eventos de auditoria podem envolver muitas mudanças, como as que envolvem mudança de definição de agente. Nesses casos, pode ser difícil identificar em XML o que mudou no evento de auditoria.

Para ajudar com isso, a ferramenta de auditoria inclui apoio para uma ferramenta de comparação de sua escolha que você use para comparar o estado do evento antes que seja mudado.



Para configurar o apoio de ferramenta de comparação de auditoria

1. Clique em **Ferramentas > Administração > Auditoria**.
2. Na barra de ferramentas de auditoria, clique em **Enter configuração de comparação de ferramenta.**
3. Entre e **compare o caminho da ferramenta** com a sua ferramenta executável.
4. Personalize a linha de comando para sua ferramenta de comparação se necessário. %1 dos dados originais dos eventos de auditoria selecionados e 2% são os atuais dados do evento de auditoria XML selecionada. Você deve incluir ambos o 1% e o 2% dos parâmetros para que a comparação funcione.
5. Clique em **Salvar.**

Para ver as diferenças de dados XML no evento de auditoria.

1. Clique duas vezes no evento de auditoria que você quer checar as diferenças.
2. Na caixa de diálogo **Detalhes da entrada de auditoria,** clique no botão **Diferenças.**
3. Veja as diferenças na ferramenta de comparação que você configurou.

Criando filtros para consultas de evento de auditoria

O histórico do evento de auditoria é exibido na ferramenta (**Ferramentas > Administração > Auditoria**). Você deve ter a função de configuração de auditoria ou de auditor para ver essa ferramenta no console.

Você pode criar filtros para consultas de auditoria personalizadas. Você pode escolher a partir dos seguintes filtros de auditoria:

- **Nome de usuário:** Mostra eventos de auditoria para o nome do usuário especificado.
- **Nome do dispositivo:** Mostra eventos de auditoria para um nome de dispositivo especificado.
- **Data modificada:** Mostra eventos de auditoria entre uma série de datas especificadas ou dentro de um número de dias especificado.
- **Características:** Mostra eventos de auditoria para as características selecionadas. Você deve selecionar as **Características** antes que você possa expandir o circuito de **Eventos**.

Se você selecionar filtros múltiplos eles serão dúvidas E opções. Por exemplo, se você selecionar um nome de usuário e uma característica, os resultados mostrarão somente dispositivos que correspondem a ambos nome do usuário e aquela característica.

Para criar uma consulta de auditoria personalizada

1. Clique em **Ferramentas > Administração > Auditoria**.
2. Clique no item **Consultas personalizadas**
3. Clique no botão da barra de ferramentas **Definição da nova consulta.**
4. Modifique os filtros que desejar.
5. Ao terminar, clique em **Criar.**

Relatórios

Uso de relatórios

A ferramenta de relatórios pode ser usada para gerar uma grande variedade de relatórios detalhados, que fornecem informações críticas sobre os dispositivos gerenciados na sua rede. Essa ferramenta relatório aproveita as vantagens do utilitário de análise de inventário Management Suite, que coleta e organiza dados de hardware e software a fim de produzir relatórios úteis, informativos e atualizados.

Vários tipos de relatórios estão disponíveis:

- **Relatórios padrão (pré-definidos):** Relatórios padrão que acompanham o Management Suite.
- **Relatórios personalizados:** Os relatórios personalizados que definem um conjunto exclusivo de informações para gerar um relatório. Você também pode personalizar todos os relatórios padrão usando o Designer de relatórios de Data Dynamics.
- **Relatórios ad hoc:** Relatórios de um clique disponíveis de várias áreas do Management Suite. Por exemplo, você pode clicar com o botão direito e em **Novo relatório** para gerar um relatório baseado na consulta.

Você pode agendar relatórios para que sejam executados em um intervalo regular. Relatórios agendados podem ser publicados e gravados em um arquivo seguro em um local compartilhado no servidor núcleo, onde qualquer pessoa com credenciais de login apropriadas podem acessar e exibir relatórios. Você também pode agendar para que os relatórios publicados sejam enviados por e-mail para destinatários designados.

Para iniciar a ferramentas Relatórios

Clique em **Ferramentas > Relatórios/Monitoração > Relatórios**.

Para usar relatórios no Web console

Clique em **Relatórios** no grupo **Relatórios**.

Grupos de relatórios

Abra a ferramenta Relatórios para acessar relatórios predefinidos.

Os relatórios são organizados em uma estrutura de árvore, agrupado nas seguintes pastas:

- **Meus relatórios:** Relatórios que o usuário atual criou ou copiou de outra pasta. Esses são, em geral, relatórios que você pode executar regularmente e organizar para seu próprio uso. Você pode criar pastas para organizar os relatórios. O administrador tem acesso a cada um dos grupos de relatórios do usuário e pode adicionar e remover relatórios.
- **Relatórios padrão:** Relatórios pré-definidos são instalados com o Management Suite. Os relatórios pré-formatados têm propriedades de consulta e tipos de gráficos atribuídos e estão prontos para serem usados.
- **Relatórios públicos:** Relatórios personalizados disponibilizados para todos os usuários no servidor núcleo.
- **Todos os relatórios:** Todos os relatórios que podem ser usados pelo usuário atual. Esta visualização inclui um campo de busca que filtra a lista de relatórios quando você digita strings e seleciona uma coluna. (Por exemplo, digite "licença" e seleciona a coluna "Descrição" para exibir relatórios relacionados à licenças de software).

Os Administradores podem ver o conteúdo de todos os grupos de relatórios. Os usuários com o direito Relatórios também podem ver e executar relatórios e publicá-los, mas apenas nos dispositivos que fazem parte do seu escopo. Usuários com permissão para usar o Report designer podem criar relatórios personalizados.

Os relatórios são executados em relação ao escopo e permissões do usuário atualmente conectado. Se um operador não tem permissões usar uma ferramenta, este operador não pode executar relatórios que incluem essa ferramenta. Da mesma forma, os únicos dispositivos que aparecem em um relatório são aqueles incluídos em um escopo de usuário.

Fontes de relatório

Relatórios predefinidos reúnem dados do banco de dados Management Suite. Se você cria um relatório personalizado, você pode especificar outras fontes de dados disponíveis para serem incluídas no relatório.

Formatos de relatórios

Ao executar um relatório, você pode salvá-lo usando um dos formatos a seguir:

- **HTML:** HTML padrão. Você pode clicar em gráficos em relatórios de HTML para exibir informações detalhadas sobre um item.
- **Imagem:** Arquivo de imagem bitmap
- **PDF:** Arquivo do Adobe PDF
- **XML:** Arquivo de texto em formato XML
- **DOC:** Microsoft Word
- **XLS:** Microsoft Excel

Ao agendar um relatório na ferramenta Relatórios, você pode usar os seguintes formatos:

- **PDF:** Arquivo do Adobe PDF
- **XLS:** Microsoft Excel
- **DOC:** Microsoft Word
- **CSV:** Arquivo de texto de valor separado por vírgula

Recursos extras para relatórios

Para obter mais informações sobre o uso dos relatórios Management Suite, visite o portal LANDesk User Community em community.landesk.com/ldmsreports. O portal de relatórios contém documentos adicionais, consultas de clientes e relatórios para download. Qualquer usuário da LANDesk pode submeter um relatório personalizado para compartilhar com a comunidade.

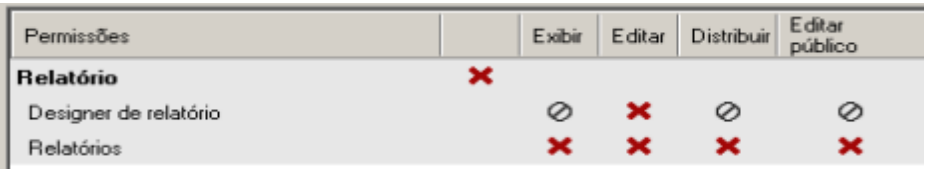
Para abrir rapidamente abrir o portal de relatórios da comunidade LANDesk User Community, vá para **Ferramentas> Relatórios/Monitoração> Relatórios** da Comunidade.

Direitos exigidos para uso de relatórios

Nem todos os usuários podem ver, poder editar e distribuir relatórios. Os usuários devem ter as permissões corretas atribuídas na Administração com base em funções. Porque a edição de relatórios envolve o acesso a base de dados, qualquer usuário com permissões de edição devem ser qualificadas para editar o banco de dados. Você também pode definir credenciais com permissões de somente-leitura para o banco de dados, caso você queira que usuários emitam relatórios sem editá-los.

Relatórios e administração baseada em funções.

A Administração com base em funções incluí permissões de Relatórios, para determinar quais usuários podem visualizar, executar, modificar, agendar e criar relatórios. Na ferramenta Gerenciamento de usuários, ao criar ou editar uma função você pode habilitar ou desabilitar as permissões de relatórios a seguir.



Permissões		Exibir	Editar	Distribuir	Editar público
Relatório	✖				
Designer de relatório		⊘	✖	⊘	⊘
Relatórios		✖	✖	✖	✖

Designer de relatório

- Sem direitos: Não pode abrir o designer.
- Editar: Pode abrir o designer e criar ou editar relatórios.

Relatórios

- Sem direitos: Não pode visualizar a ferramenta.
- Exibir: Pode visualizar esta ferramenta e relatórios. Pode executar relatórios. Não pode alterar nada.
- Editar: Pode visualizar e alterar as propriedades do relatório. Esta permissão não dá acesso ao designer. A permissão editar é necessária para acessar o Report designer.
- Distribuir: Pode programar e poder publicar relatórios.
- Editar público: Pode mover relatórios para a pasta Pública.

Permissões de usuário para banco de dados de relatórios

O Report designer é uma ferramenta poderosa que deve ser usada com cautela. Usuários com permissão para editar o designer de relatórios podem acessar qualquer parte do banco de dados e executar qualquer comando de SQL, logo, certifique-se que os usuários com essa permissão sejam qualificados para gerenciar o banco de dados. Dados podem ser perdidos ou corrompidos se um usuário executar comandos de SQL que modifiquem dados.

A ferramenta Relatórios acessa o banco de dados com as credenciais do usuário que foram especificadas durante a instalação do produto. Essas credenciais podem ser gerenciadas na caixa de diálogo **Configurar serviços do Software LANDesk** Se você preferir definir credenciais diferentes para usuários com permissões relatórios, você pode criar um segundo conjunto de credenciais para acesso ao banco de dados de relatórios.

Por exemplo, se você quiser que os usuários dos relatórios tenham acesso 'somente leitura', você pode criar uma conta de usuário de banco de dados.com acesso somente leitura. Em seguida, você inseriria essa conta de usuário como o usuário do banco de dados Relatórios na caixa de diálogo **Configurar serviços do Software LANDesk**.

NOTA: Se você estiver usando um banco de dados Oracle e criar um usuário de relatórios somente leitura, você precisará .criar um sinônimo público para cada tabela referenciada em relatórios por este usuário.

Tópicos relacionados

"Criar um usuário com direitos de relatórios" na página 200

Criar um usuário com direitos de relatórios

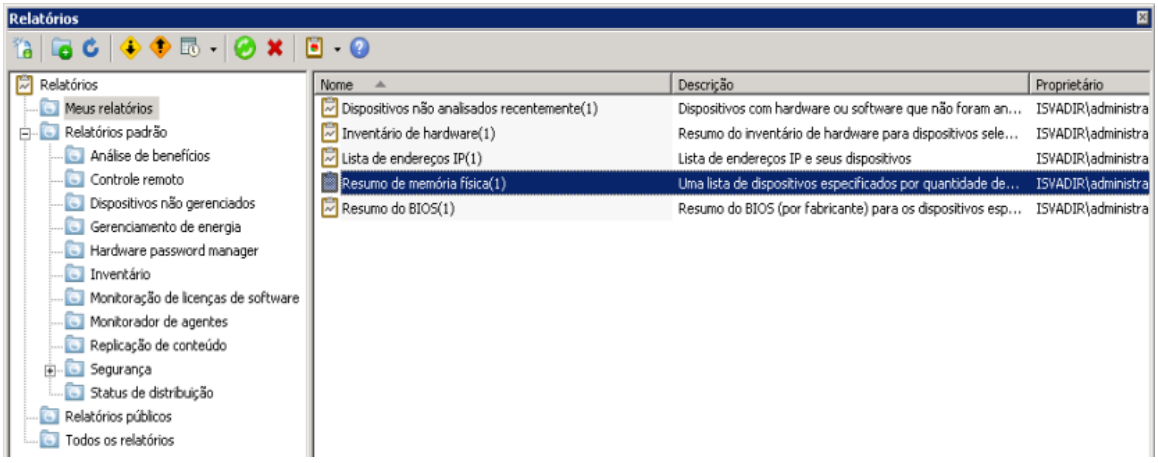
A ferramenta Relatórios acessa o banco de dados com as credenciais do usuário que foram especificadas durante a instalação do produto. Se você preferir definir credenciais diferentes para usuários com permissões relatórios, você pode criar um segundo conjunto de credenciais para acesso ao banco de dados de relatórios.

Para especificar credenciais para usuários de banco de dados de relatórios

1. Crie uma conta de usuário para seu banco de dados, atribuindo as permissões desejadas.
2. No console Management Suite, clique em **Configurar > Serviços**
3. Em **Usuário de banco de dados relatórios** , digite o nome de usuário e senha da conta.
4. Clique em **OK**.

Execução de relatórios

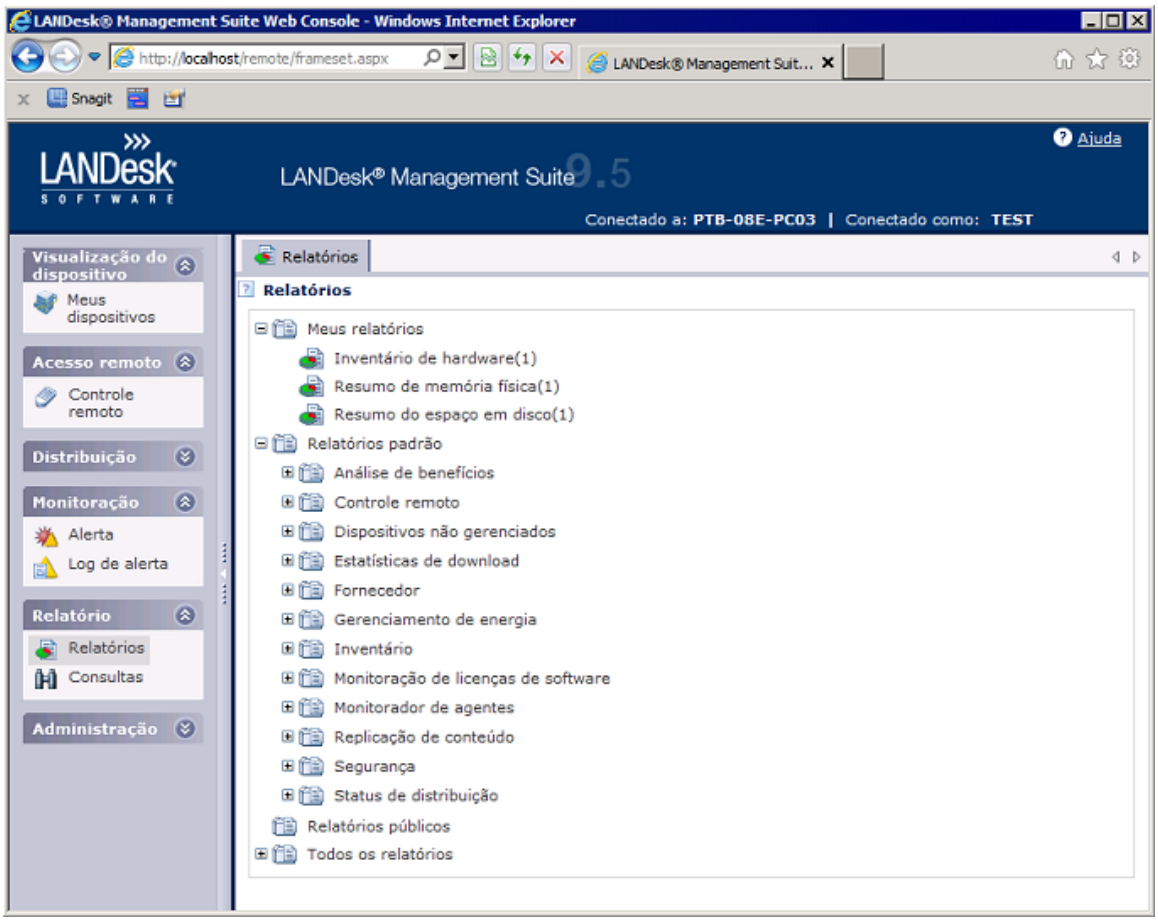
Use a ferramenta Relatórios para executar relatórios, organizá-los e criar novos. Você pode programar relatórios para serem executados uma ou repetidas vezes. Você também pode importar e exportar relatórios para uso em outros consoles do Management Suite.



A forma mais rápida de exibir dados e a execução de relatórios a partir de um console. O visualizador de relatórios exibe os dados como uma pré-visualização da página impressa ou como dados contínuo. Você pode mudar as exibições e formatos no visualizador. Você também pode mudar os parâmetros de relatório para selecionar um subconjunto dos dados.

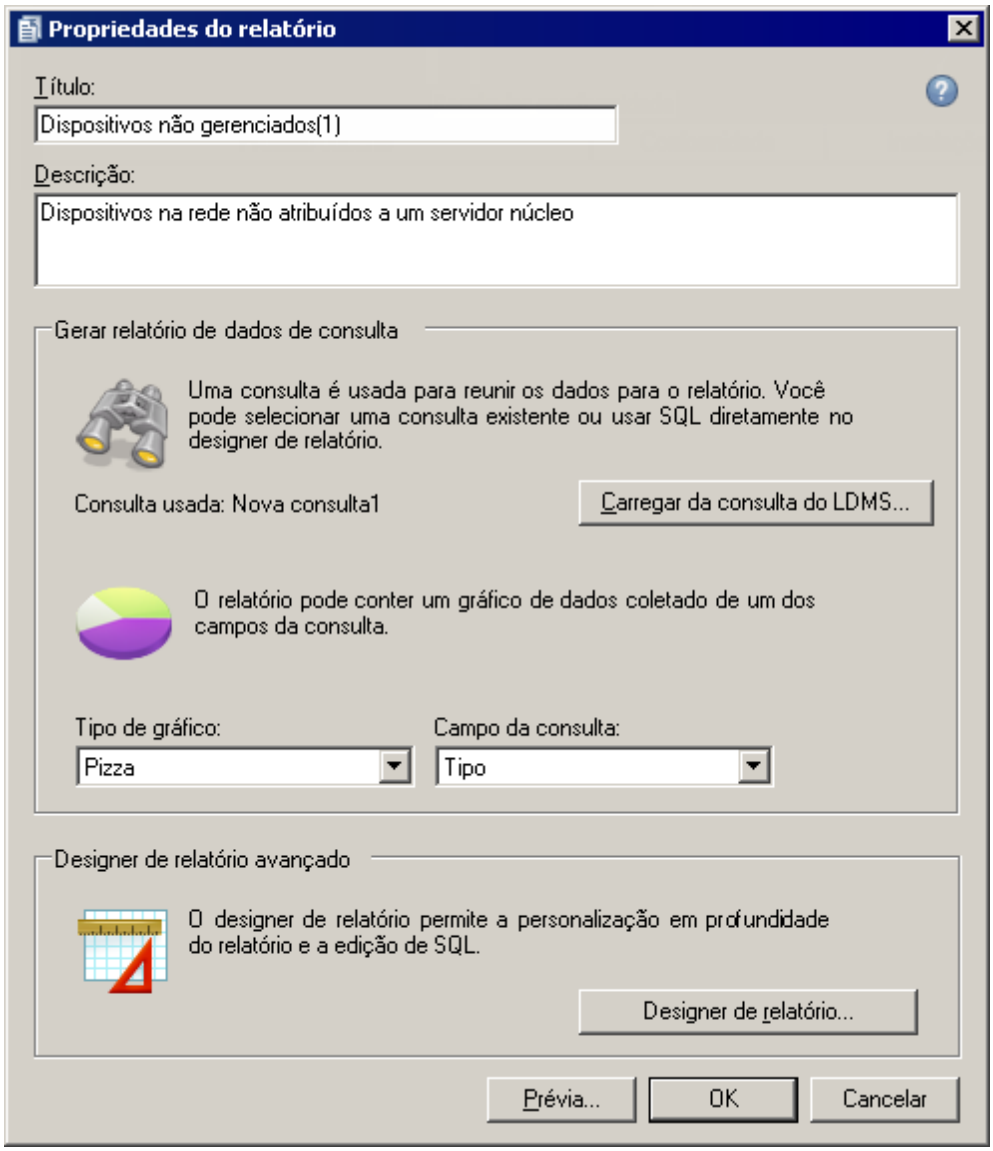
Relatórios no console Web

Ao usar o Web console, os relatórios encontrados no console do Windows estão disponíveis, mas existem pequenas diferenças na forma de exibição e seleção de parâmetros selecionados. Você não pode editar nem criar um relatório personalizado no Web console, nem mover relatórios entre pastas, mas você pode executar, exibir e exportar relatórios.



Mudar propriedade de relatórios

Você pode fazer uma cópia de um relatório predefinido e modificar itens na caixa de diálogo **Propriedades de relatório**. Você pode mudar o tipo de gráfico exibido no relatório e especificar um campo de consulta diferente como o elemento chave da consulta. Você também pode selecionar uma consulta LDMS para usar como base do relatório. Você também pode mudar o nome e descrição.


Propriedades do relatório
Título:
Dispositivos não gerenciados(1)
Descrição:
Dispositivos na rede não atribuídos a um servidor núcleo
Gerar relatório de dados de consulta
Uma consulta é usada para reunir os dados para o relatório. Você pode selecionar uma consulta existente ou usar SQL diretamente no designer de relatório.
Consulta usada: Nova consulta1
Carregar da consulta do LDMS...
O relatório pode conter um gráfico de dados coletado de um dos campos da consulta.
Tipo de gráfico:
Pizza
Campo da consulta:
Tipo
Designer de relatório avançado
O designer de relatório permite a personalização em profundidade do relatório e a edição de SQL.
Designer de relatório...
Prévia...
OK
Cancelar

Se você quiser fazer mudanças mais extensas ao relatório, você deverá abrir o Designer de relatórios.

See "Criação de relatórios personalizados" on page 213 para obter detalhes sobre como usar o desenhista de relatório.

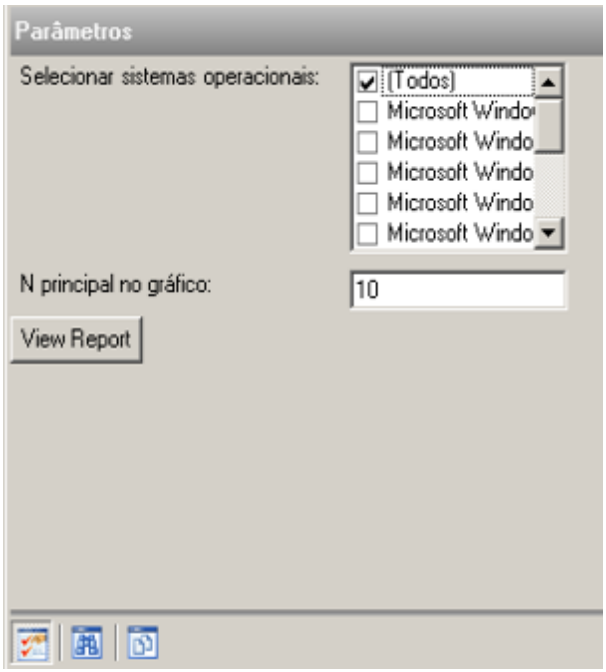
Visualizador de relatórios

Ao executar um relatório, o visualizador de relatórios é executado e exibe o relatório gerado. Esse visualizador de relatórios permite a exibição dos relatórios da forma que você preferir. A partir do visualizador de relatórios você também pode exportar um relatório ou salvá-lo em um formato diferente para distribuição.

O visualizador de relatórios inclui uma barra de ferramentas e uma barra lateral. As barras de ferramentas contem os seguintes botões:

- **Abrir:** Abra um relatório no visualizador.
- **Exportar:** Exceto o relatório como uma imagem (formatos BMP, EMF, GIF, JPEG, TIFF ou PNG) ou HTML, PDF, XML, XLS ou DOC.
- **Copiar:** Copia o conteúdo do relatório para a página selecionada.
- **Visualizar impressão:** Alterna entre os modos de impressão e de visualização. Se não estiver selecionado, o relatório é exibido com um única página em HTML.
- **Configurar página:** Altera as configurações de página, layout e marcas d'água.
- **Imprimir:** Abre a caixa de diálogo da impressora padrão.
- **Painel da barra lateral:** Ativa o painel da barra lateral, que exibe opções de busca, parâmetros e a visualização de miniaturas.
- **Retornar ao relatório pai:** Se você está visualizando um sub-relatório, volte ao relatório pai que gerou o sub-relatório exibido.
- **Nenhum:** Use o mouse normalmente para visualização.
- **Modo panorâmico:** Arraste o ponteiro em formato de mão para obter uma vista panorâmica em qualquer direção na página.
- **Modo de seleção:** Arraste o ponteiro para selecionar uma nova porção da página. Você pode colar a seleção em outro aplicativo compatível com o texto colado.
- **Modo de captura instantânea:** Arraste o ponteiro para selecionar um retângulo. Você pode colar o retângulo em outro aplicativo compatível com a colagem de imagens.
- **Zoom para perto:** Aumenta o tamanho do relatório.
- **Zoom para longe:** Diminui o tamanho do relatório.
- **Porcentagem do zoom:** Selecione o tamanho do modo de visualização do relatório.
- **Primeira página:** Exibe a primeira página do relatório.
- **Página anterior:** Exibe a página anterior em ordem sequêncial.
- **Caixa de página:** Insere um número específico de página, que permite ir direto para a página especificada.
- **Página seguinte:** Veja a próxima página, em ordem sequencial.
- **Última página:** Veja a última página do relatório.
- **Cancelar:** Interrompe a execução do relatório. Se a execução do relatório estiver concluída, este botão aparece esmaecido.
- **Atualizar:** Retorna à visualização inicial.
- **Localizar:** Abre o painel de pesquisa para procurar uma linha específica de texto.

A barra lateral inclui três opções, acessados nos ícones na parte inferior da barra lateral:



- **Parâmetros:** Muda os parâmetros do relatório para selecionar um sub-conjunto de dados e alternar os resultados conforme a definição do relatório. Uma vez que diferentes parâmetros diferentes estiverem selecionados, clique em **Exibir relatório** para atualizar o relatório com os novos parâmetros.
- **Pesquisar resultado:** Pesquisa um conjunto de caracteres no resultado do relatório. Especifique conjunto de caracteres e selecione algum critério (por exemplo, diferenciar maiúsc./minusc.) e clique em **Pesquisar**. Uma lista de ocorrências são exibidas. Clique em uma ocorrência para ir para essa seção do relatório. A ocorrência é destacada. Você também pode clicar em uma barra verde ao lado direito do relatório para mover entre ocorrências.
- **Miniaturas de páginas:** Exibir miniaturas das páginas do relatório. Clique em uma miniatura para ir para a página correspondente.

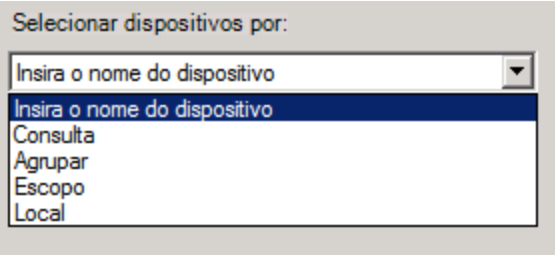
Selecionar parâmetros de uma lista

Quando a barra lateral incluir uma lista com parâmetros, você pode incluir todos os itens da lista no relatório selecionando a caixa de seleção **Todos**. Ao fazer isto, as caixas de seleção de cada item não são selecionadas, mas todos serão incluídos no relatório.

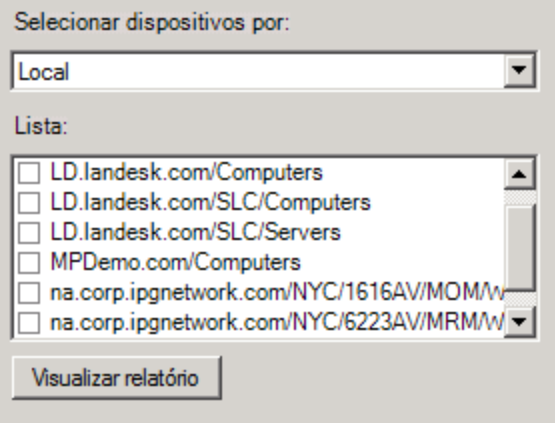
Para selecionar um subconjunto de itens, desmarque a caixa de seleção **Todas** e marque as caixas de seleção ao lado de cada item que você deseja incluir no relatório.

Selecionar dispositivos, grupos ou locais

Os parâmetros variam com cada relatório. No entanto, todos os relatórios incluem uma opção de seleção de dispositivo que especifica dispositivos individuais, consultas, grupos, escope ou localização. Isso deixa você gerar um relatório para uma consulta, grupos ou escopo que você definiu na tela de rede ou para uma local na rede.



Por exemplo, você pode selecionar dispositivos em um local baseado no local do dispositivo de rede. Ao selecionar a Localização, a lista exibe os locais na rede classificada pelo nome do domínio.



Sub relatórios

Alguns relatórios podem abrir relatórios secundários ou sub-relatórios. Na pasta de Segurança existem relatórios no estilo relatório gerencial para Antivírus e Vulnerabilidades. Se você abrir o relatório gerencial (ou relatório pai), você pode clicar em um dos gráficos para abrir o sub-relatório correspondente (ou relatório filho).

Por exemplo, se você executar o relatório gerencial Antivírus, clique no gráfico "Status da verificação em tempo real" para abrir um relatório separado com o status do dispositivo de verificação. Você pode clicar no botão **Voltar ao relatório pai** para retornar ao relatório do dashboard.

Execute um relatório

Ao executar um relatório, o visualizador de relatórios exibe os dados como uma pré-visualização da página impressa ou como dados contínuo. Você pode mudar as exibições e formatos no visualizador. Você também pode mudar os parâmetros de relatório para selecionar um subconjunto dos dados.

1. Na ferramenta **Relatórios**, selecione uma pasta na estrutura de árvores dos Relatórios e procure o relatório desejado.
2. Clique duas vezes no relatório.

   A caixa de diálogo pré-visualização de relatório é exibida. Alguns relatórios têm parâmetros configuráveis que permitem que você selecione um subconjunto de dados para o relatório. Se não houver parâmetros padrão, você precisa inserir ao menos um (por exemplo, especificar um nome de dispositivo) ou o relatório estará em branco.

3. Se houver parâmetros para escolha, especifique os parâmetros desejados.

4. Clique em **Exibir relatório**.
5. Para exibir detalhes de qualquer parte de um gráfico, clique na área do gráfico. A exibição muda para a seção do relatório com os dados representados nessa área do gráfico.
6. Nas páginas de relatórios, clique nas setas das no cabeçalhos das colunas para classificar dados por aquela coluna.
7. Use os botões na barra de ferramentas procurar dados, exportá-los em um formato diferente, imprimir o relatório e assim por diante.
8. Ao concluir, feche a janela de navegação do visualizador.

NOTA: Ao selecionar dispositivos usando o parâmetro Dispositivo, nenhum caractere curinga é usado. Digite qualquer número de caracteres comuns no nome do dispositivo que você deseja selecionar e clique **Exibir relatório**. Todos os nomes de dispositivos com esse conjunto de caracteres será incluído no relatório.

Selecionar parâmetros de uma lista

Quando a barra lateral incluir uma lista com parâmetros, você pode incluir todos os itens da lista no relatório selecionando a caixa de seleção **Todos**. Ao fazer isto, as caixas de seleção de cada item não são selecionadas, mas todos serão incluídos no relatório.

Para selecionar um subconjunto de itens, desmarque a caixa de seleção **Todas** e marque as caixas de seleção ao lado de cada item que você deseja incluir no relatório.

Salvar um relatório como arquivo

Depois de executar um relatório, você pode salvar os resultados em uma localização de arquivo. O relatório pode ser salvo como imagem (formatos BMP, EMF, GIF, JPEG, TIFF ou PNG) ou nos formatos TML, PDF, XML, XLS, ou DOC.

1. Execute um relatório
2. Na barra de ferramentas do visualizador, clique no botão **Exportar**.
3. Clique no formato de relatório desejado.
4. Na caixa de diálogo **Exportar**, mude os parâmetros do relatório. (Os parâmetros variam dependendo do formato que você selecionou).
5. Vá até o local onde você quer salvar o relatório, digite o nome do relatório eclique em **Salvar**.
6. Clique em **Exportar**.

NOTA: Se você salvar um relatório e pretender enviá-lo por e-mail, use o formato PDF no lugar do HTML.

Agendamento de relatórios

Se houver um relatório que precisa regularmente, você pode agendá-lo com antecedência para execução ou fora do expediente quando a carga do banco de dados núcleo pode estar mais leve. Um relatório agendado é salvo na pasta compartilhada de relatórios da LANDesk (ldmain\relatórios) e também é enviado aos usuários do servidor núcleo com permissões de Relatório e que possuam um endereço de e-mail associado com seu nome de usuário (na ferramenta Gerenciamento de usuários). O envio de relatórios por e-mail requer um servidor SMTP de e-mail.

Um relatório salvo fora da pasta compartilhada de Relatórios (ldmain\relatórios) é baseado no escopo da pessoa que o agendou. No caso de relatórios enviados para outros destinatários, o relatório usa o escopo de cada destinatário para filtrar os dados.

Para agendar um relatório, um usuário deve ter a permissão Distribuição de relatórios.

Se você quiser distribuir um relatório que você executou, salve o relatório no formato desejado e anexe-o a uma mensagem de e-mail. O relatório usará seu alcance. Os usuários com permissão a pasta compartilhada de relatórios também podem visualizar o relatório a partir dessa pasta.

NOTA: Se você salvar um relatório e pretender enviá-lo por e-mail, use o formato PDF no lugar do HTML.

NOTA: Relatórios em execução com uma grande volume de dados podem consumir uma grande quantidade de recursos de sistema no servidor núcleo. Por causa disso, só é possível agendar um relatório de cada vez. Se um relatório corre e você programa outros relatórios ao mesmo tempo, os segundos relatórios subseqüentes serão atrasados até que o primeiro relatório completou.

Agendar um relatório

1. Na ferramenta **Relatórios**, expanda a árvore e selecione um relatório para agendar.
2. Clique **Agendar** na barra de ferramentas e selecione o formato desejado.

   A ferramenta **Tarefas agendadas** são exibidas com o relatório selecionado.

3. Clique no botão **Propriedades** na barra de ferramentas.
4. Na caixa de diálogo **Agendar tarefa**, digite ou edite as informações em todas as páginas.
5. Clique em **Salvar**.

Você pode ver o andamento do relatório na ferramenta Tarefas agendadas (clique na pasta **Minhas tarefas**).

Para descrições das opções na caixa de diálogo Agendar tarefa consulte "Sobre a caixa de diálogo Agendar tarefa" na página 225.

Modificar propriedades de relatórios

1. Na ferramentas **Relatórios**, copie um relatório e cole a cópia em um poster.
2. Clique com o botão direito e selecione **Propriedades**.
3. Na caixa de diálogo **Propriedades do relatório**, altere qualquer propriedades.
4. Clique em **Visualizar** para exibir o relatório personalizado no visualizador de relatório.
5. Clique em **OK** para salvar o relatório modificado.

Personalizar um modelo de relatório

Todos os relatórios são baseados em modelos fornecidos junto com o Management Suite da LANDesk. Se você quiser personalizar um modelo de relatório, você deve abrir o arquivo mestre de modelos no designer de relatórios. Por exemplo, você pode querer adicionar o nome da sua empresa e a logo ao modelo, ou mudar o layout básico da página, fonte ou outros elementos.

Existem três arquivos de modelo, um com orientação retrato, um paisagem e um para modelos de painel gerencial.

NOTA: Os modelos de relatório são instalados em todos os dispositivos onde você instalar um console. Se você muda um modelo no servidor núcleo, ele será usado quando você executar relatórios no núcleo e a partir do console da Web. No entanto, outros consoles usarão o modelo que foi instalado. Se você quiser usar o modelo revisado em outros consoles, você deverá copiar o arquivo modelo para cada console adicional ou criar uma tarefa para distribuir os modelos.

Para personalizar um modelo de relatório

1. Na ferramenta **Relatórios**, clique no botão **Editar modelo** na barra de ferramentas.
2. Selecione a opção retrato, paisagem ou relatório gerencial.

   O modelo abre no designer de relatórios.

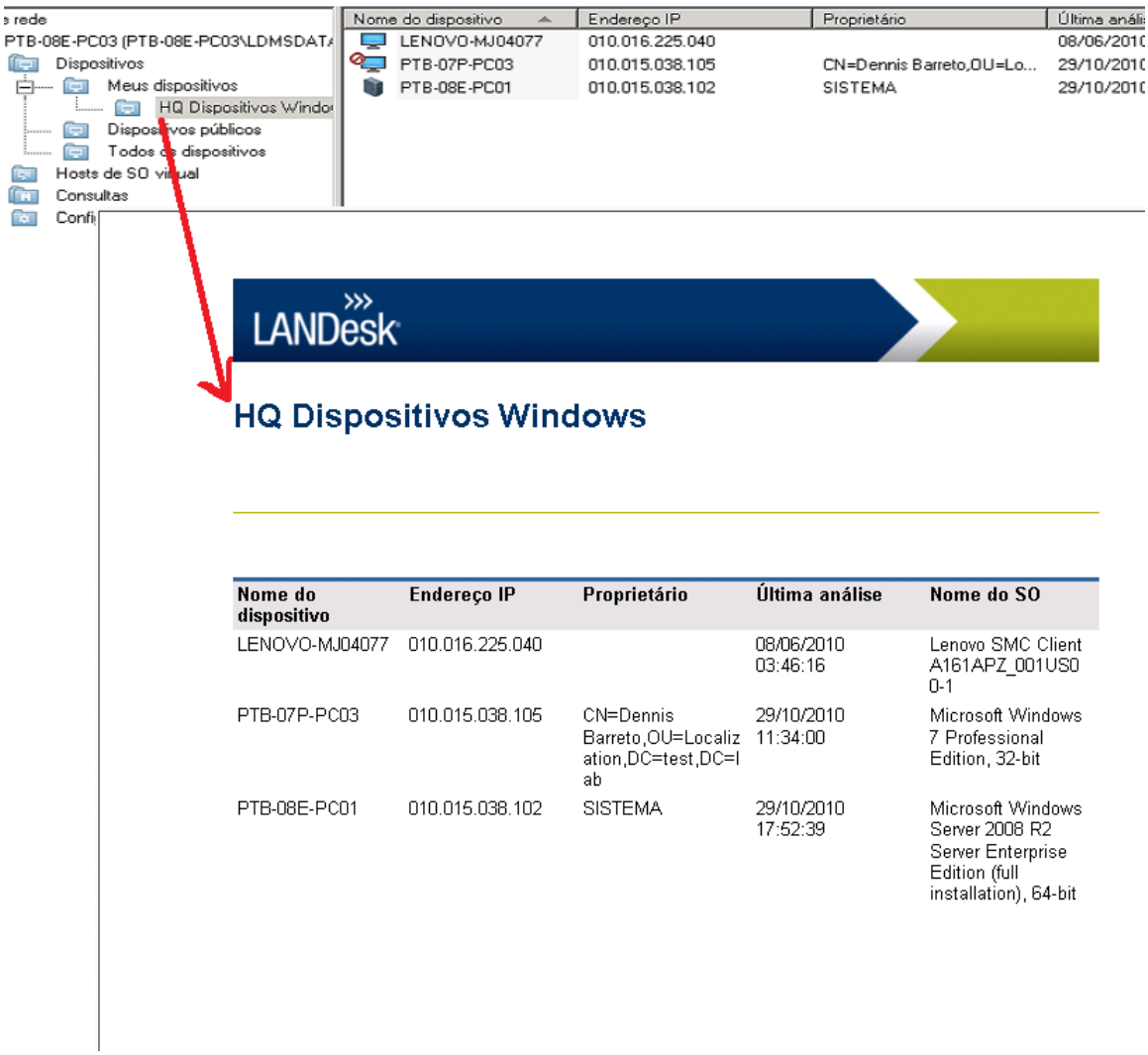
3. Faça as alterações desejadas no designer de relatórios. Ao terminar, clique no botão **Salvar** na barra de ferramentas.

Executar relatórios ad hoc

Relatórios simples estão disponíveis para a maioria de itens no console de Windows. Qualquer grupo ou recipiente (tal como uma consulta) tem a opção de execução do relatório no menu de contexto. O relatório exibe os dados no modo de exibição atual, organizados usando as colunas de dados exibidas no console.

Por exemplo, um relatório ad hoc de um grupo na Tela de rede lista os dispositivos daquele grupo. As colunas no modo de exibição redes (como endereço IP, proprietário e assim por diante) são exibidas no relatório. Para mudar a organização dos dados de relatório, ajuste as colunas (adicione ou retire colunas, ou altere sua ordem) antes de executar o relatório.

Você pode executar um relatório para várias ferramentas, exibindo os itens de uma forma exclusiva (tal como uma lista de conjuntos de regras na ferramenta Alertas). Você pode executar um relatório para qualquer consulta ou grupo que você criou no modo de exibição redes ou em outro lugar.



Existem três formas de criar relatórios rapidamente a partir do console:

- **Exibir como relatório:** Clique com o botão direito em um item e selecione esta opção para exibir os dados em um formato padrão de relatório. Uma janela de pré-visualização relatório é exibida e você pode selecionar diversas opções antes de imprimir, salvar ou enviar o relatório.
- **Exportar como CSV:** Clique com o botão direito nesta opção para salvar os dados em arquivo .csv.
- **Novo relatório:** Clique com o botão direito em uma consulta e selecione esta opção para criar um novo relatório baseado na consulta. Você pode usar um formato padrão ou abrir o designer para personalizar o relatório mais tarde. O novo relatório será salvo em Meus relatórios.

Executar um relatório ad hoc

Relatórios simples estão disponíveis para a maioria de itens no console de Windows. Qualquer grupo ou recipiente (tal como uma consulta) tem a opção de execução do relatório no menu de contexto. O relatório exibe os dados no modo de exibição atual, organizados usando as colunas de dados exibidas no console.

1. No console do Windows, clique com o botão direito no item da árvore, como em um grupo no modo de exibição Redes ou em um item no painel de ferramentas.
2. Se houver um item de menu **Exibir como relatório**, clique nele e selecione o formato de relatório desejado.

Se **Exibir como relatório** não existir no menu, o item que você selecionou com o botão da direita não é compatível com esta opção.

Salvar um relatório como um arquivo CSV

Você pode salvar dados como um arquivo CSV (valores separados por vírgula) para a maioria dos itens no console do Windows. Itens com este recurso tem uma opção de menu de contexto que salva dados de relatório neste formato.

1. No console do Windows, clique com o botão direito no item da árvore, como em um grupo no modo de exibição Redes ou em um item no painel de ferramentas.
2. Selecione **Exportar como CSV** e especifique um local para salvar o arquivo CSV.

Se a opção **Exportar como CSV** não existir no menu, o item que você selecionou não é compatível com esta opção.

Criar um relatório a partir de uma consulta

Você pode executar um relatório para qualquer consulta ou grupo que você criou no modo de exibição redes ou em outro lugar.

1. Clique com o botão da direita no modo de exibição redes.
2. Clique no item de menu **Novo relatório**.
3. Digite um nome e descrição para o relatório e faça quaisquer outras alterações personalizadas que você desejar.
4. Clique em **OK** para salvar o relatório.

Se o item **Novo relatório** não existir no menu, o item que você selecionou com o botão da direita não é compatível com esta opção.

Organização de relatórios

Ao usar relatórios padrão e criar relatórios personalizados, você deverá organizá-los e modificá-los para que atendam as suas necessidades.

Copiar e modificar

Relatórios padrão não podem ser excluídos, mas podem ser copiados e colados em outras pastas. Por exemplo, você pode criar uma pasta em **Meus relatórios** que contenha os relatórios que você usa com maior frequência.

Você também pode copiar um relatório padrão, edita-lo e salvá-lo como um relatório exclusivo. Isto é geralmente mais fácil do que criar um relatório desde o início. Cada vez você copia um relatório, um número é anexado ao nome do relatório para distingui-lo de outras cópias. Ao editar um relatório você pode renomeá-lo com um nome exclusivo.

NOTA: Você deve fazer uma cópia em separado de um relatório para cada revisão criada. Se você copiou e alterou um relatório, depois fez outras alterações e salvou-o novamente, as modificações anteriores serão perdidas. Recomendamos que você faça uma nova cópia cada vez que alterar um relatório, para garantir que consultas ou parâmetros não sejam perdidos.

Compartilhar com outros servidor núcleo

Os relatórios são executados usando uma base de dados do servidor núcleo. Se você tem múltiplos servidores núcleo, você pode compartilhar relatórios entre eles para que os relatórios sejam padronizados na empresa.

Compartilhe um relatório somente uma vez usando a opção **Copiar para outros núcleos**. Isto salva uma cópia de um relatório na mesma estrutura de pasta da outra ferramenta de relatórios do servidor núcleo.

Para compartilhar um relatório de forma permanente, você pode sincronizar relatórios entre servidores núcleo. Sempre que um relatório é modificado, uma cópia do relatório modificado é automaticamente gravada em outros servidores núcleos que você selecionou para sincronização de conteúdo. Este recurso faz parte da ferramenta **Sincronização de núcleo**.

Importar e exportar

Você pode importar e exportar relatórios, para salvar cópias de seus relatórios ou para compartilhar relatórios e modelos com outros. Por exemplo, se você grava cópias exportadas de seus relatórios e excluiu um relatório, porém, mais tarde decide que o quer de volta, você pode importá-lo novamente.

Os relatórios são armazenados em arquivos de texto XML com uma extensão .ldms no local que você especificar. Esses arquivos só podem ser lidos por LANDesk Management Suite.

Os nomes da pasta e do arquivo exportado são geralmente os mesmos que aparecem na ferramenta relatórios.

Copiar, mover e excluir relatórios

Você também pode copiar qualquer relatório, editá-lo e salvá-lo como um relatório exclusivo. Isto é geralmente mais fácil do que criar um relatório desde o início. Ao copiar um relatório, um número é anexado ao nome do relatório para distingui-lo de outras cópias. Ao editar um relatório você pode renomeá-lo com um nome exclusivo.

NOTA: Você deve fazer uma cópia em separado de um relatório para cada revisão criada. Se você copiou e alterou um relatório, depois fez outras alterações e salvou-o novamente, as modificações anteriores serão perdidas. Recomendamos que você faça uma nova cópia cada vez que alterar um relatório, para garantir que consultas ou parâmetros não sejam perdidos.

Para copiar e mover relatórios

1. Clique em **Ferramentas > Relatórios/Monitoramento > Relatórios**.
2. Expanda a estrutura de árvore para encontrar o relatório desejado.
3. Arraste o relatório para outra pasta.

NOTA: Embora você possa copiar e colar todos os tipos de relatórios, somente os relatórios

personalizados ou copiados podem ser copiados e colados. Para fazer isto, clique com o botão direito no relatório e selecione **Recortar**, então abra a pasta de destino, clique com o botão direito e clique em **Colar**.

Para excluir um relatório

1. Clique em **Ferramentas > Relatórios/Monitoramento > Relatórios**.
2. Expanda a estrutura de árvore para encontrar o relatório desejado.
3. Selecione um relatório e clique no botão **Excluir** na barra de ferramentas.

Somente relatórios personalizados ou copiados podem ser excluídos.

Sincronizar relatórios entre servidores núcleo

Os relatórios podem ser sincronizados entre diversos servidores núcleo. Com a sincronização do núcleo, é possível copiar configurações e tarefas de um núcleo a outro, manual ou automaticamente. A sincronização permite que você copie itens regularmente e garante que servidores núcleo múltiplos usem as mesmas ferramentas e dados.

1. Clique em **Ferramentas > Administração > Sincronização de núcleo**.
2. Em **Componentes**, clique com o botão direito em **Relatórios** e selecione **Sincronização automática.**

Para sincronizar um relatório com outros núcleos, clique com o botão direito no relatório e clique em **Sincronização automática**.

Tópicos relacionados

"Sincronização do núcleo" na página 92

Copiar relatórios para outros servidores núcleo

Sincronize um relatório sobre encomenda com a opção **Copiar para outro núcleo**. Ao fazer isso, você pode selecionar os servidores que deseja que recebam a cópia. A cópia só ocorre uma vez e o item que você copiou fica disponível imediatamente nos núcleos remotos.

1. Na ferramenta **Relatórios**, expanda a árvore e selecione um relatório para copiar. Use Ctrl+ ou Shift+ para selecionar vários relatórios.
2. Clique com o botão direito no relatório e selecione **Copiar para outros núcleos.**
3. Selecione os servidores núcleo dos quais você deseja receber uma cópia.
4. Clique em **Copiar conteúdo** para iniciar a cópia imediatamente.

Observe que você pode precisar atualizar manualmente a tela do console do núcleo pressionando **F5** para o item aparecer. As cópias remotas têm o mesmo nome e local da cópia de origem e são editáveis. Os grupos ou subgrupos que contêm o item serão criados automaticamente.

Importar e exportar relatórios

Os relatórios são armazenados em arquivos de texto XML com uma extensão .ldms no local que você especificar. Esses arquivos só podem ser lidos por LANDesk Management Suite.

Os nomes da pasta e do arquivo exportado são geralmente os mesmos que aparecem na ferramenta relatórios.

Para exportar um relatório

1. Na ferramenta **Relatórios**, expanda a árvore e selecione um relatório para exporta.
2. Na barra de ferramentas, clique no botão **Exportar**.
3. Vá ao local aonde você deseja exportar o relatório e clique em **Salvar**.

Para importar um relatório

1. Na ferramentas **Relatórios**, selecione a pasta para a qual você quer importar relatórios (Meus relatórios ou Relatórios públicos).
2. Na barra de ferramentas, clique no botão **Importar**.
3. Vá até o local do relatório para onde você deseja importar e clique em **Abrir**.
4. Na caixa de diálogo **Opções de Importação**, selecione uma opção de importação.
    - **Atualizar:** Adiciona relatórios aos grupos especificados no. arquivo .ldms, mantendo a mesma identificação. Se o relatório já existe não é duplicado.
    - **Inserir itens nos grupo ou proprietário selecionado:** Adiciona relatórios ao grupo selecionado, designa uma nova identificação, e atualiza o proprietário. Se o relatório já existir, uma segunda cópia é salva com um número de versão no nome.
    - **Inserir itens em grupos especificados no arquivo .ldms:** Adiciona relatórios aos grupos especificados no arquivo .ldms e designa uma nova identificação. Se o relatório já existir, uma segunda cópia é salva com um número de versão no nome.
5. Clique no botão **Importar**.

Criação de relatórios personalizados

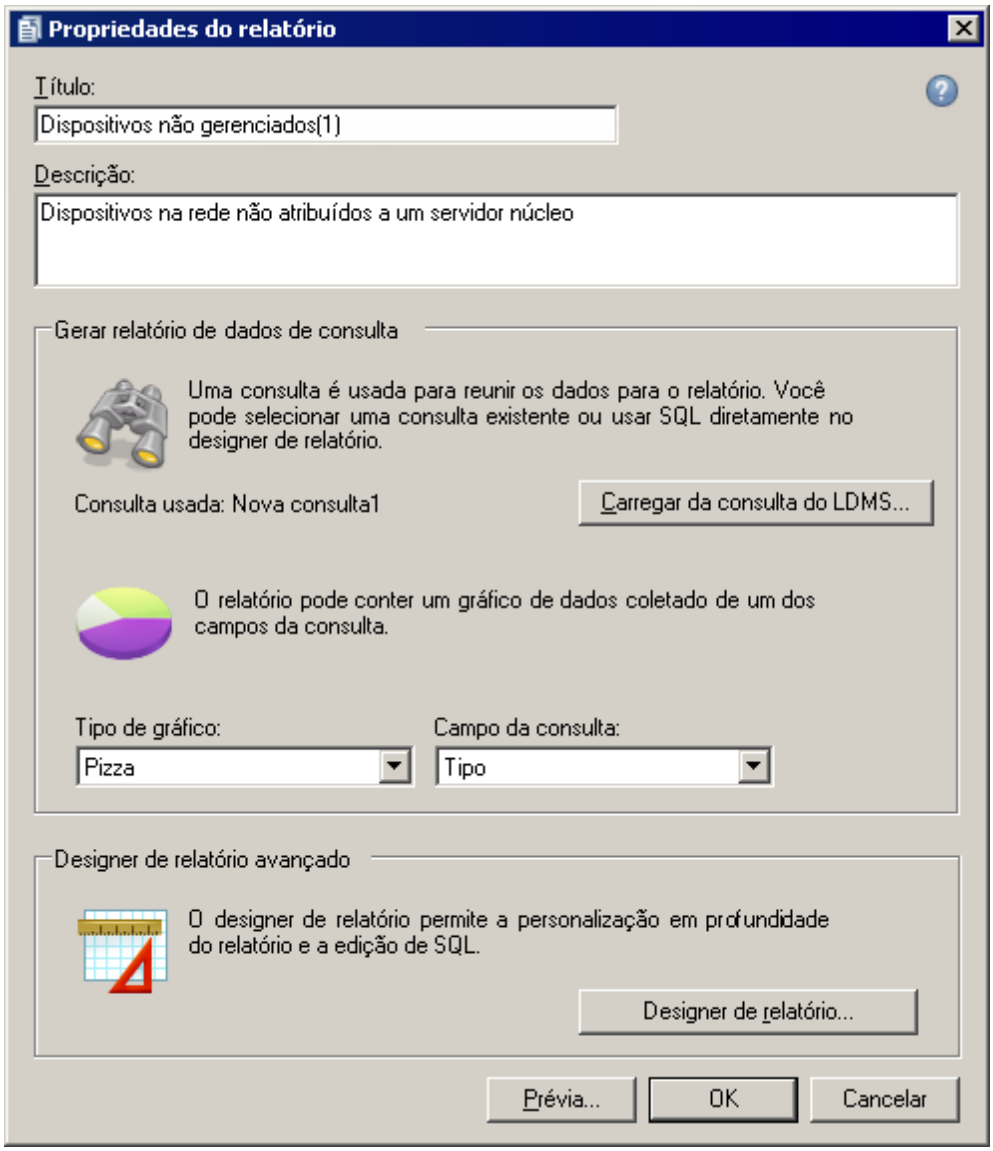
A ferramentas Relatórios tem um designer integrado Data Dynamics que permite o controle total de todos os aspectos dos relatórios. No designer você usa elementos de layout de página vinculados aos objetos de dados para exibir os dados selecionados. Você pode personalizar a aparência do relatório, instruções adjacentes de consulta SQL, os parâmetros disponíveis aos usuários e assim por diante.

Você pode criar ou modificar um relatório com uma das ações a seguir:

- Copie um relatório padrão, cole em Meus relatórios e edite-o.
- Crie uma consulta no Management Suite e use essa consulta como a base para um relatório.
- Crie um novo relatório usando fontes de dados, parâmetros, instruções SQL, elementos de layout de página e imagens.

Propriedades de relatório

Ao criar ou editar um relatório, as propriedades são as primeiras a serem especificadas.


Propriedades do relatório
Título:
Dispositivos não gerenciados(1)
Descrição:
Dispositivos na rede não atribuídos a um servidor núcleo
Gerar relatório de dados de consulta
Uma consulta é usada para reunir os dados para o relatório. Você pode selecionar uma consulta existente ou usar SQL diretamente no designer de relatório.
Consulta usada: Nova consulta1
Carregar da consulta do LDMS...
O relatório pode conter um gráfico de dados coletado de um dos campos da consulta.
Tipo de gráfico:
Pizza
Campo da consulta:
Tipo
Designer de relatório avançado
O designer de relatório permite a personalização em profundidade do relatório e a edição de SQL.
Designer de relatório...
Prévia...
OK
Cancelar

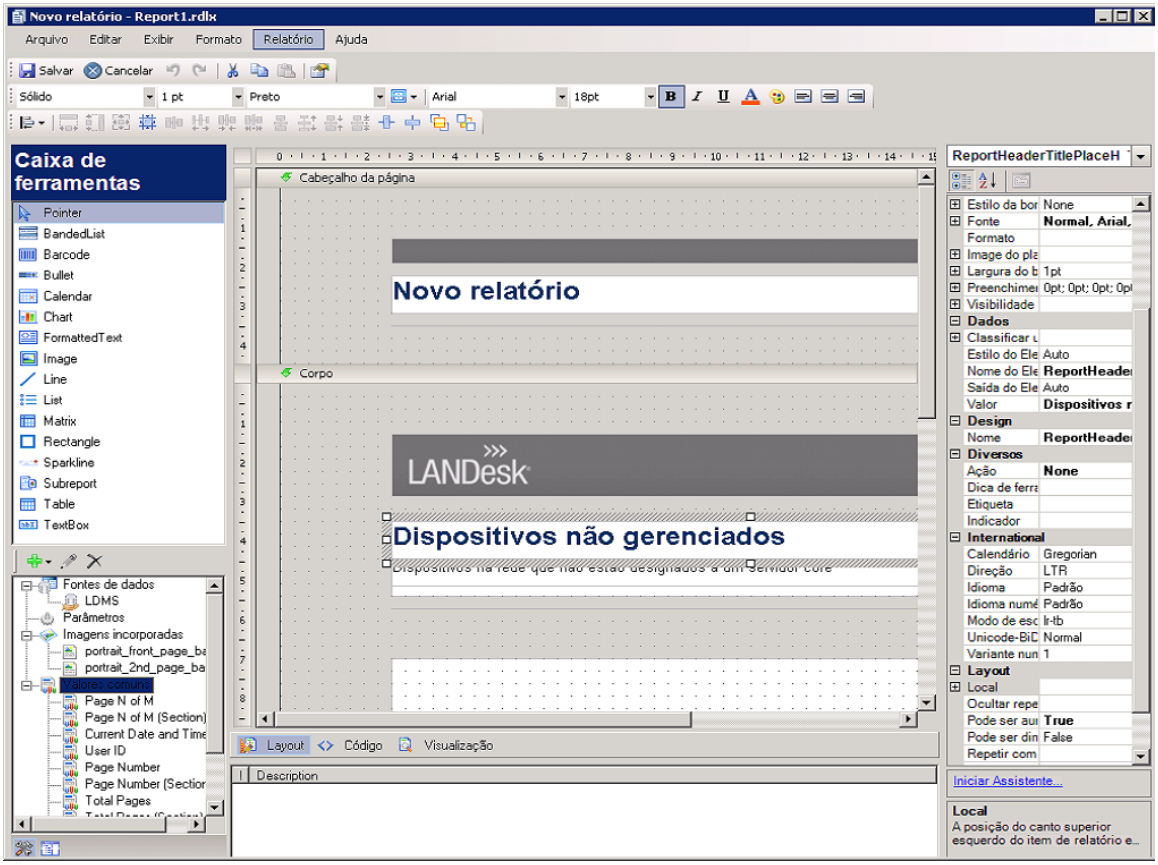
- **Título:** Digite um nome descritivo para o relatório.
- **Descrição:** Adicione outras informações descritivas para o relatório.
- **Carregue da partir de consulta do LDMS:** Selecione uma consulta do Management Suite e use-a como a base para um novo relatório.
- **Tipo de gráfico:** Selecione um estilo de gráfico (pizza ou barras).
- **Campo de consulta:** Especifique quais campos do relatório estão representados no gráfico.
- **Designer de relatório:** Abra o aplicativo designer de relatório para fazer mudanças detalhadas nos dados e layout do relatório. (Se este botão estiver esmaecido, o usuário não tem permissão para uso do Report Designer)
- **Visualizar:** Visualize o relatório com as opções que você selecionou nesta caixa de diálogo.

Se você copiou um relatório padrão, você pode simplesmente alterar itens na caixa de diálogo de Propriedades e salvar o novo relatório. Mas é mais provável que você queira abrir o designer de relatórios e fazer alterações mais substanciais.

Designer de relatório

A partir da caixa de diálogo de propriedades do relatório você pode abrir o designer de relatório. Um aplicativo separado, o Data Dynamics Reports, é integrado com a ferramentas Relatórios e a banco de dados.

NOTA: Para abrir o designer de relatório um usuário deve ter permissão de edição no Report designer.



O designer de relatório permite o acesso a todos os aspectos de um relatório.

- **Layout de página:** O centro do designer exibe o design da página do relatório. Clique no botão **Visualização** abaixo do layout para abrir o visualizador de relatório e ver como o relatório será depois de executado.
- **Caixa de ferramentas** Arraste uma ferramenta sobre a página para inserir o objeto.
- **Descrição do documento:** Veja a descrição do relatório na coluna a esquerda (no lugar da caixa de ferramentas).
- **Fonte de dados:** Especifique as fontes de dados que você deseja usar ao executar o relatório. Defina a fonte dos dados e então adicione conjunto de dados (consultas) e parâmetros que você usará no relatório.
- **Parâmetros:** Defina parâmetros que determinem os resultados de relatório.
- **Propriedades:** A coluna da direita exibe propriedades do objeto selecionado que podem ser editadas.

- **Assistente:** Clique em **Executar o assistente** para exibir todas as propriedades do objeto selecionado, organizado por tipo de opção.

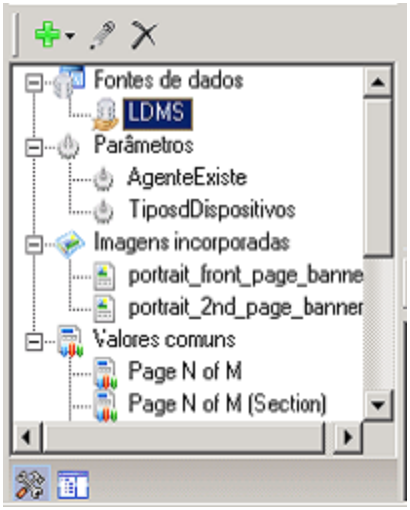
Noções básicas sobre a criação e edição de relatórios

O designer de relatórios é uma ferramenta flexível e cheia de recursos, que dá opções de consulta e exibição de dados a partir de diversas fontes. Ao criar um relatório, você necessita dos seguintes itens básicos:

- Uma fonte de dados e conjuntos definidos de dados a partir dos quais o relatório é povoado
- Um layout de página para visualização dos dados.
- As regiões de dados e outros itens de relatório que formatam os dados

As fontes e conjunto de dados

Os relatórios extraem informações da *fonte de dados*, um banco de dados usando um formato padrão tal como SQL, ODBC, Oracle, ou XML. A fonte de dados é definida junto com os *conjuntos de dados*, que são consultas mencionadas no relatório. O Explorer de dados, localizado ao lado esquerdo do designer exibe as fontes de dados e conjunto de dados em um modo de exibição de árvore. No exemplo abaixo, o LDMS é a fonte de dados (o banco de dados do Management Suite) e os Dispositivos do Windows são os jogos de dados. O nome e versão são os nomes de campos (tabelas de banco de dados) mencionados na consulta ao banco de dados.

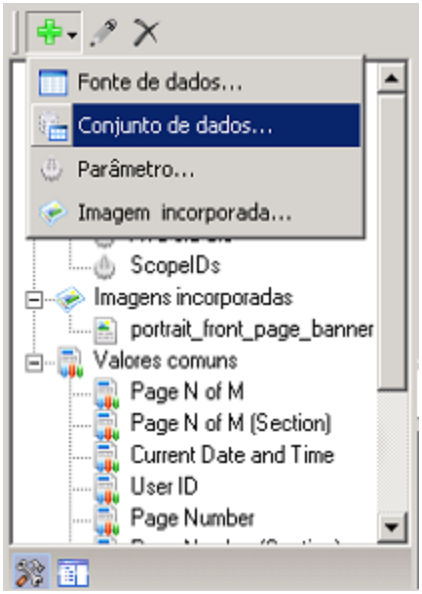


O banco de dados do Management Suite aparece como uma fonte de dados padrão quando você cria um novo relatório. Você pode adicionar qualquer outra fonte, basta especificar o tipo de dado, uma string de conexão e as credenciais necessárias para acessar os dados. Isto permite que os dados sejam extraídos não somente do banco de dados do Management Suite, mas de qualquer outra fonte, assim como quando você cria um relatório personalizado.

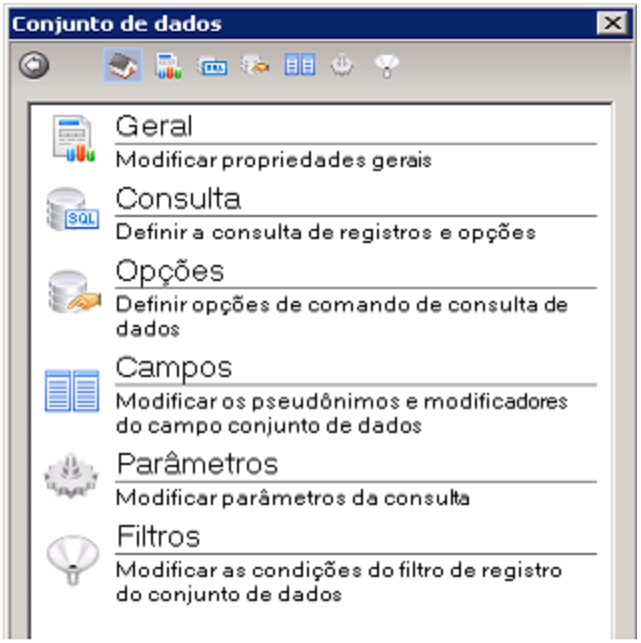
Os parâmetros passam as informações entre os conjuntos de dados. No visualizador de relatório, os parâmetros podem ser exibidos para deixar o usuário refinar a seleção de dados exibidos.

Adicionar elementos de dados

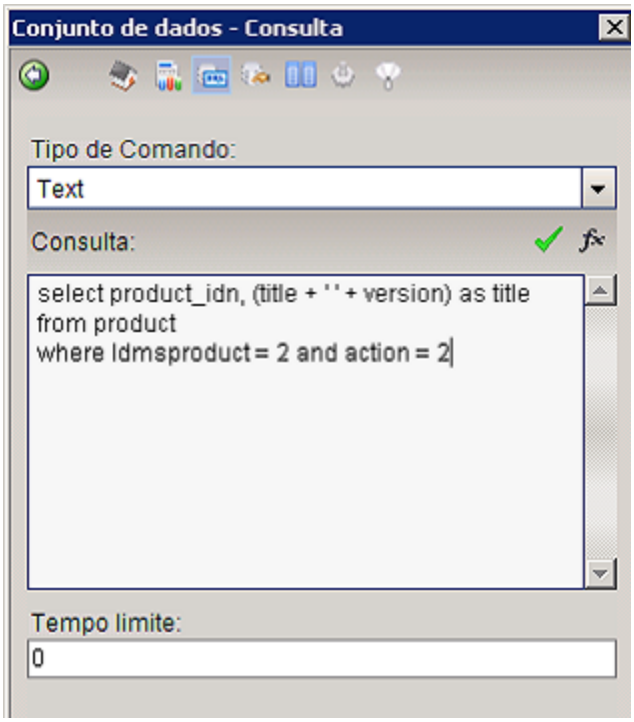
O designer de relatório inclui assistentes para ajudar no vínculo de fonte de dados e na definição de conjuntos de dados e parâmetros. Por exemplo, quando você clica em uma fonte de dados (tal como o LDMS), clique no botão **Adicionar** e selecione **Conjunto de dados**.



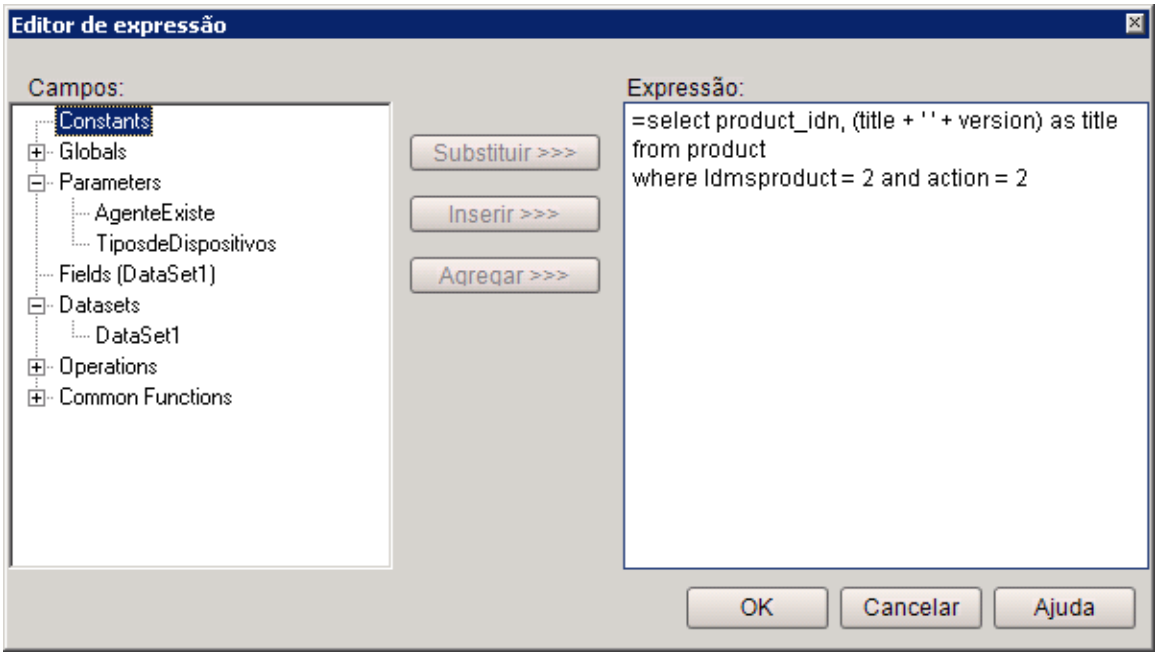
O assistente de conjunto de dados é exibido com propriedades organizadas em seis grupos.


Conjunto de dados
Geral
Modificar propriedades gerais
Consulta
Definir a consulta de registros e opções
Opções
Definir opções de comando de consulta de dados
Campos
Modificar os pseudônimos e modificadores do campo conjunto de dados
Parâmetros
Modificar parâmetros da consulta
Filtros
Modificar as condições do filtro de registro do conjunto de dados

Na página de consulta do assistente, por exemplo, você pode adicionar uma consulta SQL. Clique na marca verde para verificar a sintaxe e clique no símbolo função (*fx*) para abrir o editor de expressão.

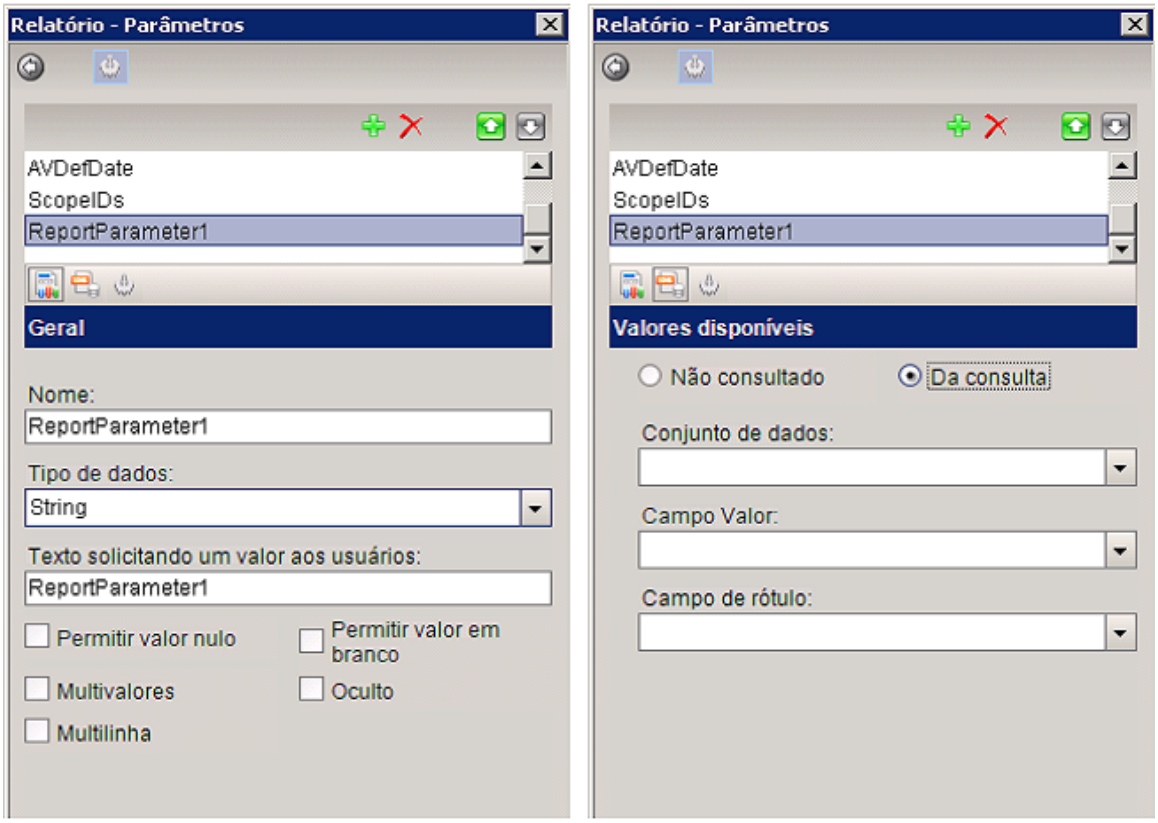


O editor de expressão lista todos os campos disponível para o elemento selecionado e permite que você insira esses itens (por exemplo, parâmetros e campos de conjuntos de dados) em uma expressão. Além dos campos relacionados aos conjuntos de dados, existem valores normalmente usados que são definidos globalmente, além de usuários padrão e funções que você pode inserir em uma expressão.

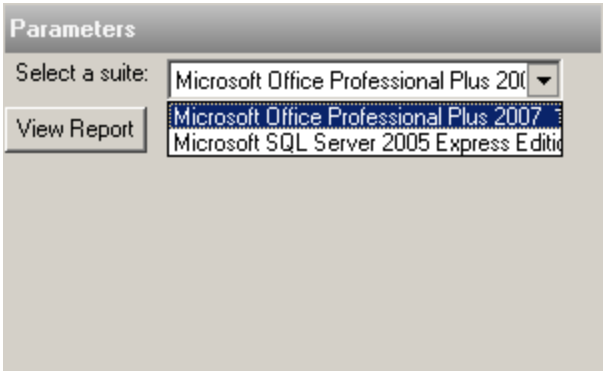


Depois de adicionar pelo menos um conjuntos de dados você pode definir os parâmetros baseados nestes conjuntos de dados. Quando um usuário executa um relatório, os parâmetros adicionados são exibidos no visualizador de relatório para que o usuário possa selecionar quais dados serão exibidos no relatório.

No exemplo a seguir, o conjunto de dados **Suites** foi criado e refere-se a tabela **produto** com os campos **product_idn**, **título** e **versão**. Um parâmetro chamado **Suite** é criado. Na página **Geral** da caixa de diálogo, o nome é adicionado e um texto informativo (Selecione um conjunto) é definido. Este é o lembrete que será exibido no visualizador de relatório. Na página **Valores disponíveis**, os valores da consulta são definidos O campo valor é **product_idn** (um número exclusivo de identificação do banco de dados) e o campo rótulo é **título**, ou seja, o título (nome) da suite é exibido.



Quando o relatório é executado, este parâmetro é exibido com uma lista que permite a seleção de um produto da suite:



A terceira página na caixa de diálogo Parâmetros permite que você especifique uma seleção padrão para o parâmetro.

Representar seleções de parâmetro em uma consulta

Quando você permite que usuários selecionem um parâmetro, você pode mencionar essa seleção em uma consulta usando uma instrução SQL exclusiva no editor de relatórios Data Dynamics: "em (?)". Essa instrução usa o valor de parâmetro atualmente selecionado enquanto o relatório é executa o relatório. Um exemplo disto é exibido na seguinte amostra de código.

A seguinte consulta usa campos das tabelas **produto** e **slm_productsuiteref** para selecionar os produtos que estão incluídos na suite de produtos. Neste caso, uma única suite de produtos é incluída, identificada por seu número de identificação (615).

```
select p.product_idn, p.title, p.version de slm_productsuiteref r
left outer join product p on p.product_idn = r.product_idn where r.productsuite_idn = 615
ordenar por p.title
```

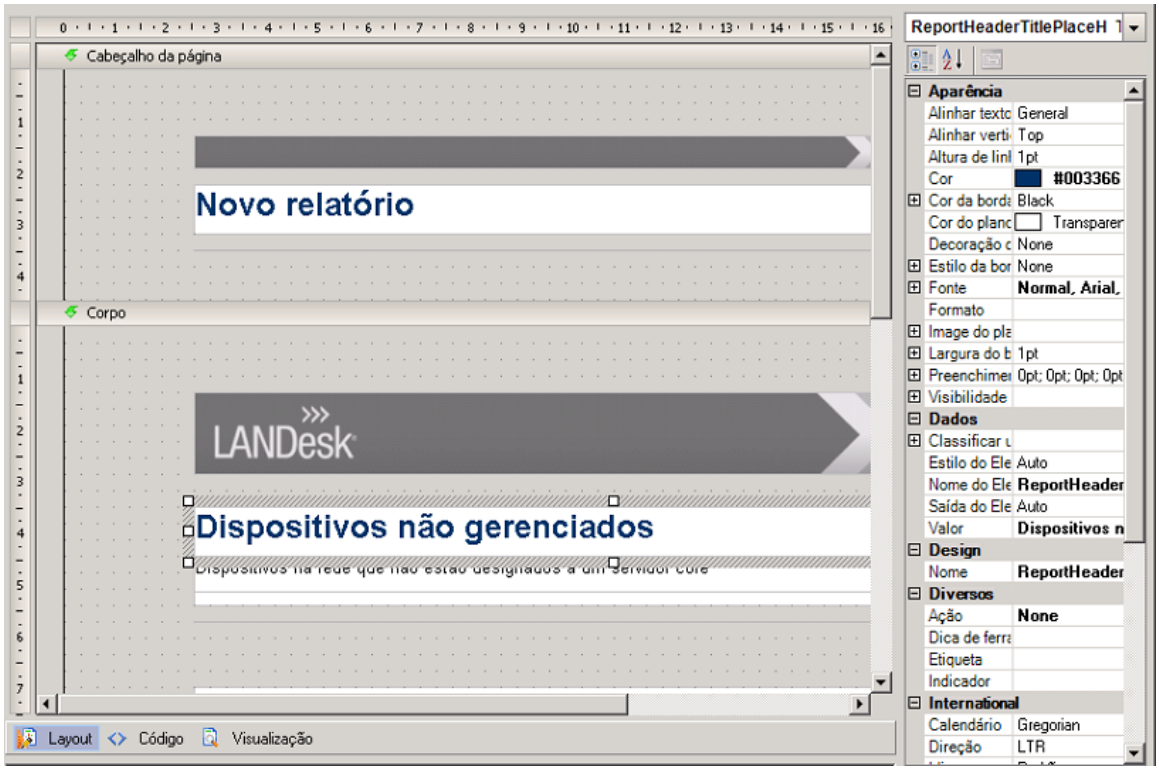
Em vez de especificar uma suite, você pode substituir a referência específica a suite de produtos com " em (?)" para incluir a suite que o usuário seleciona ao executar o relatório.

```
select p.product_idn, p.title, p.version de slm_productsuiteref r
left outer join product p on p.product_idn = r.product_idn where r.productsuite_idn in (?)
ordenar por p.title
```

Você achará outros exemplos deste uso em alguns Relatórios padrão que exigem que o usuário selecione um valor de parâmetro.

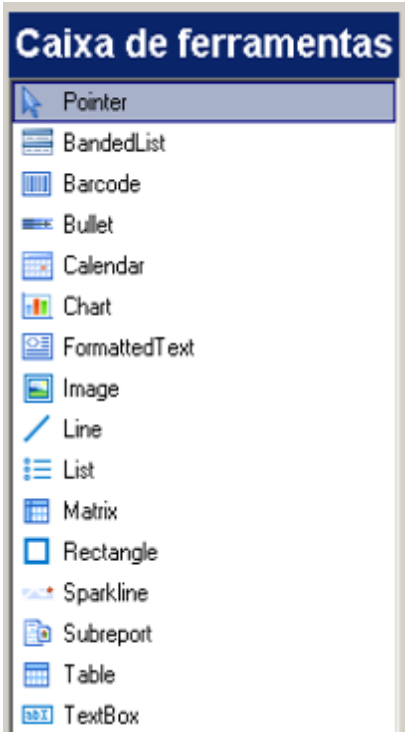
Layout

Os layouts de relatório definem o formato de emissão da página, usando tamanhos normais de página. Você pode especificar o tamanho, orientação, cabeçalho e rodapé e o formato do corpo do relatório.



Os relatórios padrão usam um cabeçalho com o logotipo da LANDesk que é suprimido na página 1. O layout de corpo começa com uma logo maior que só aparece uma vez, enquanto os dados abaixo do logotipo preenche tantas páginas quanto necessário.

Enquanto você trabalha no layout da página, você pode adicionar elementos de formatação e de região de dados rapidamente arrastando ferramentas da caixa de ferramentas.



Arraste um item sobre o layout, e depois mova e redimensione. Defina o objeto em detalhes usando o painel de propriedades (ao lado direito do editor), ou clique em **Abrir assistente** para editar as mesmas propriedades com a ajuda do assistente, com itens agrupados por tipo de propriedade.

Regiões de dados

Os dados são formatados usando *regiões de dados*, que são elementos de formato padrão definidos para tipos específicos de exibições. As regiões de dados incluem:

- **Tabelas:** Linhas e colunas, com um campo de um conjunto de dados para cada coluna. Você também pode agrupar as linhas por um campo, assim como pode agrupar dados por dispositivo, onde você tem uma linha de cabeçalho para cada dispositivo e dados de apoio agrupados abaixo do cabeçalho. (Veja o relatório Inventários de hardware para obter um exemplo de linhas agrupadas).
- **Lista:** Os itens são repetidos em uma lista para cada registro na fonte de dados. Você pode usar qualquer tipo de formatação para listas, e, para agrupamentos complexos você pode aninhar listas ou colocar uma lista dentro de outra região de dados.
- **Lista aninhadas:** Uma coleção de faixas (cabeçalho, detalhe e rodapé) onde os dados são repetidos na faixa de detalhes. Listas aninhadas são uteis porque você pode inserir elementos livremente sem estar limitado por formatos de tabela ou lista.
- **Matriz:** Também linhas e colunas, mas formatadas com os dois cabeçalhos, de coluna e de linha, como uma tabela de referência cruzada ou dinâmica.

As regiões de dados estão incluídas na caixa de ferramentas. Elas podem ser combinadas, aninhadas e incluídas em outros elementos de layout.

Itens de relatórios

Os itens na caixa de ferramentas são usados para formatar o layout de página e inserir dados na página.

- **Aslinhas** são usadas para formatar o visual.
- **Os retângulos** são um elemento visual que contém outros itens.
- **As caixas de texto** podem ser usadas para inserir texto estático ou ou dados dinâmicos em qualquer lugar na página.
- As **Imagens** podem ser colocadas em qualquer lugar na página.
- **Os gráficos** apresentam um resumo dos dados selecionados.
- Os **Códigos de barra** podem renderizar dados em 23 estilos de códigos de barra.
- **Mini-gráficos** são pequenos gráficos que resumem os dados e podem ser inseridos no texto.
- **Os calendários** podem ser adicionados a uma página e vinculados aos dados para exibir eventos dentro de uma faixa de datas.

Estes e outros elementos são completamente personalizáveis e podem ser combinados de várias maneiras para agrupar e exibir dados.

Para idéias sobre como você pode definir seus próprios relatórios, veja as propriedades de qualquer relatório padrão e clique em **Designer de relatórios** para ver como o relatório foi definido.

Ajuda adicional

Para obter uma ajuda detalhada sobre o designer de relatórios, visite o site da comunidade LANDesk (community.landesk.com). As informações também estão disponíveis no site da Data Dynamics Reports (datadynamics.com).

Uso de relatórios [Web Console]

Ao usar o Web console, todos relatórios encontrados no console do Windows estão disponíveis, mas existem pequenas diferenças na forma de exibição e seleção de parâmetros selecionados. Você não pode editar nem criar um relatório personalizado no Web console, nem mover relatórios entre pastas, mas você pode exibir, imprimir e exportar relatórios.

Quando um usuário executa um relatório a partir do Web console, o escopo do usuário é aplicado ao relatório. O relatório conterá somente dados de dispositivos dentro do escopo do usuário.

Para usar relatório no Web console, um usuário deve ter pelo menos a permissão Relatórios - Exibir.

Para executar um relatório a partir do Web console

1. Na caixa de ferramentas do console Web, clique em **Relatórios > Relatório**s.
2. Expanda a estrutura de pastas e encontre o relatório desejado.
3. Clique no relatório.

   O relatório será exibido no visualizador em uma nova janela de navegação.

4. Selecione os parâmetros que você deseja no **Exibir relatório**.

5. Para exibir detalhes de qualquer parte de um gráfico, clique na área do gráfico. A exibição muda para a seção do relatório com os dados desejados.
6. Use os botões na barra de ferramentas procurar dados, exportá-los em um formato diferente, imprimir o relatório e assim por diante.
7. Ao concluir, feche a janela de navegação do visualizador.

Para salvar um relatório no Web console

1. Execute um relatório
2. Na barra de ferramentas do visualizador, selecione o formato de relatório desejado na lista **Selecione um formato**, em seguida, clique no botão **Exportar**.
3. Salve o arquivo usando as configurações do seu navegador.

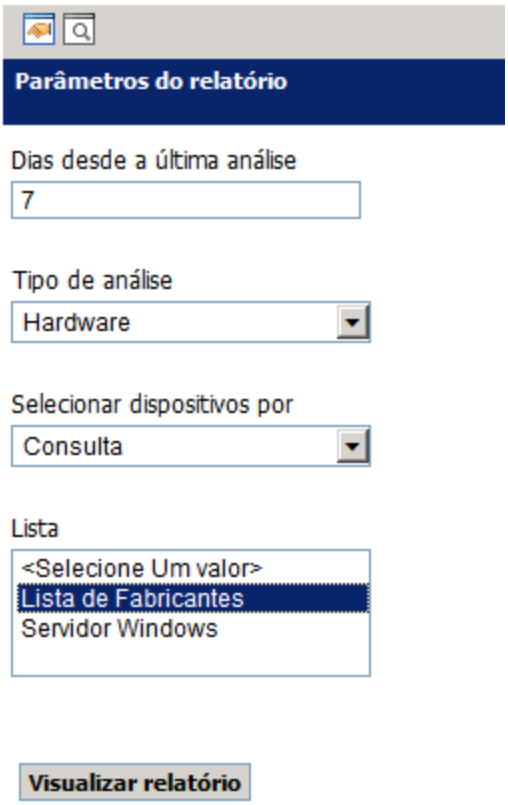
NOTA: Se você salvar um relatório e pretender enviá-lo por e-mail, use o formato PDF no lugar do HTML.

Visualizador de relatórios do Web console

O visualizador de relatório no console de Web permite que você exiba, imprima e exporte relatórios. As barras de ferramentas contém os seguintes botões:

- **Retornar ao relatório pai:** Se você está visualizando um sub-relatório, volte ao relatório pai que gerou o sub-relatório exibido.
- **Ocultar/exibir a barra lateral:** Ativa o painel da barra lateral, que exibe opções de busca, parâmetros e a visualização de mapas.
- **Configurar página:** Altera as configurações de página, orientação e de margem.
- **Imprimir:** Abre a caixa de diálogo de impressão associada com o tipo de saída escolhido.
- **Visualizar impressão:** Alterna entre os modos de impressão e de visualização. Se não estiver selecionado, o relatório é exibido com um única página em HTML.
- **Modo de visualização:** Exibir o relatório no formato HTML ou PDF. Selecione um formato a partir da lista e clique no botão **Modo de visualização** para alterar o formato.
- **Ir para a Página inicial:** Exibe a primeira página do relatório.
- **Voltar:** Exiba a próxima página, em ordem sequencial.
- **Caixa de página:** Insere um número específico de página, que permite ir direto para a página especificada.
- **Avançar:** Veja a próxima página, em ordem sequencial.
- **Ir para a Página final:** Veja a última página do relatório.
- **Selecione um formato:** Selecione o formato no qual você deseja salvar o relatório (PDF, HTML, DOC, XML, ou XLS file)
- **Exportar:** Salve o relatório no formato selecionado.

A barra lateral inclui três opções, representadas com ícones. Ao selecionar opções e seus respectivos parâmetros, o relatório é atualizado na tela.



- **Parâmetros:** Altere os parâmetros do relatório que variam entre os relatórios. Uma vez que diferentes parâmetros diferentes estiverem selecionados, clique em **Exibir relatório** para atualizar o relatório com os novos parâmetros.
- **Localizar:** Procure por um conjunto de caracteres nos resultados do relatório. Especifique conjunto de caracteres e selecione algum critério (por exemplo, diferenciar maiúsc./minusc.) e clique em **Pesquisar**. Uma lista de ocorrências são exibidas. Clique em uma ocorrência para ir para essa seção do relatório. A ocorrência é destacada.
- **Mapa do documento:** Exibe uma descrição do relatório, se houver um mapa do documento definido para o relatório. Esta opção não é exibida se não há nenhum mapa de documento. Clique em um item na lista para ir para aquele local no relatório.

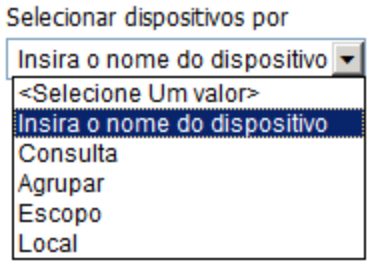
Selecionar parâmetros de uma lista

Quando a barra lateral incluir uma lista com parâmetros, você pode incluir todos os itens da lista no relatório selecionando **(Todos)**. Ao fazer isto, os itens individuais na lista não são selecionadas, mas todos serão incluídos no relatório.

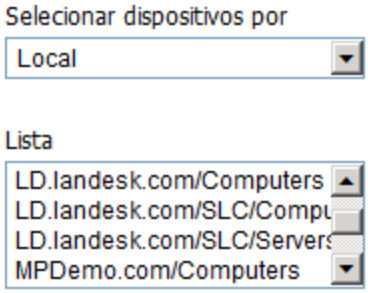
Para selecionar um subconjunto de itens, selecione todos os itens que você deseja incluir no relatório. Certifique-se que **(Todos)** não está selecionado. Use Ctrl+ clique ou Shift+ clique para selecionar vários itens, em seguida clique em **Exibir relatório**.

Selecionar dispositivos, grupos ou locais

Os parâmetros variam com cada relatório. No entanto, todos os relatórios incluem uma opção de seleção de dispositivo que especifica dispositivos individuais, consultas, grupos, escope ou localização. Isso deixa você gerar um relatório para uma consulta, grupos ou escopo que você definiu na tela de rede ou para uma local na rede.



Por exemplo, você pode selecionar dispositivos em um local baseado no local do dispositivo de rede. Ao selecionar a Localização, a lista exibe os locais na rede classificada pelo nome do domínio.



Sobre a caixa de diálogo Agendar tarefa

Ao programar um relatório, os itens a seguir podem ser configurados. Alguns itens são apenas informativos e não configuráveis.

Guia Visão geral

- **Proprietário:** O escopo do relatório corresponde ao escopo do usuário que o executa. Se você quiser escolher um usuário diferente, selecione um da lista.

Guia Agendar tarefa

- **Deixar sem agendar:** Adiciona a tarefa à janela Tarefas agendadas, mas não agenda a tarefa. Use essa opção se quiser preservar uma configuração de tarefa, mas não quiser que ela seja executada.
- **Iniciar agora:** Inicia a tarefa assim que a caixa de diálogo for fechada. Pode haver um atraso de até um minuto antes de a tarefa ser realmente iniciada.
- **Iniciar mais tarde:** Inicia a tarefa na hora e data especificadas.
- **Data e hora:** Executa a tarefa na data selecionada. Digite a data usando o formato DD/MM/AA ou clique na lista de datas para selecionar a data de um calendário.
- **Repetir a cada:** Agenda a tarefa a ser repetida periodicamente. Selecione o Dia, Semana ou Mês na lista para escolher com que freqüência a tarefa será repetida. Ela será repetida na hora definida acima.

Guia destinatários

- **Pasta de compartilhamento de relatórios da LANDesk:** Por padrão, todos os relatórios são salvos na pasta ldmain\reports, que é configurada como uma pasta compartilhada no servidor núcleo. Qualquer pessoa com permissões para esta pasta compartilhada pode abri-la e visualizar os relatórios. Se você não desejar que os relatórios sejam salvos na pasta compartilhada, desmarque esta caixa de seleção.
- **Usuários:** Marque a caixa de seleção para cada usuário que você quer que receba o relatório. Para enviar um relatório a um usuário, as propriedades do usuário devem ter um endereço de e-mail especificado (isto é feito na ferramenta **Gerenciamento de usuário**).

Guia de configuração de SMTP

- **Servidor de envio de e-mail:** Selecione o servidor SMTP que será usado para envio dos e-mails de relatórios.
- **Número da porta:** Especifique o número da porta usado pelo servidor SMTP.
- **Este servidor requer uma conexão segura:** Selecione esta caixa de seleção se o servidor SMTP exige uma conexão HTTPS.
- **Meu servidor de envio requer autenticação:** Selecione esta caixa de seleção se o servidor exigir credenciais. Você pode usar autenticação NTLM ou especificar um nome de usuário e senha.
- **Testar e-mail:** Digite um endereço de e-mail de teste e clique em **Testar** para testar as configurações do SMTP para certificar-se de que a configuração é válida.

Agendamento de tarefas

Agendamento de tarefas

O LANDesk Management Suite inclui um sistema poderoso de tarefas agendadas. O servidor núcleo e os dispositivos gerenciados têm serviços/agentes que fornecem suporte a tarefas agendadas. Os consoles do Management Suite e os consoles da Web podem adicionar tarefas ao Agendador.

Uma tarefa de distribuição de softwares consiste de um pacote de distribuição, método de entrega, dispositivos alvo e agendamento. Tarefas de não distribuição consistem no script, dispositivos alvo e horário agendado.

Aqui estão algumas tarefas que você pode agendar:

- Configurações de dispositivo
- Vários scripts personalizados
- Distribuições de formulários de dados personalizados
- Descobertas de dispositivos não gerenciados
- Análise de vulnerabilidades
- Execução de software em dispositivos gerenciados

NOTA: Os usuários do console que estarão trabalhando com scripts precisam estar no grupo LANDesk Script Writers local do servidor núcleo. Este grupo dá aos usuários do console acesso de gravação à pasta ManagementSuite\Scripts.

Gerenciamento de scripts

O LANDesk Management Suite usa scripts para executar tarefas em dispositivos. Você pode criar scripts a partir da janela **Gerenciar scripts** (**Ferramentas > Distribuição > Gerenciar scripts**).

A janela Gerenciar scripts é dividida em três categorias:

- **Meus scripts:** Scripts que você criou.
- **Scripts públicos:** Os scripts que foram marcados públicos por um usuário com direito Gerenciar scripts "Editar público". Esses scripts são do tipo apenas leitura para todos os outros usuários. Os usuários podem copiar scripts públicos para suas pastas **Meus scripts** para editá-lo.
- **Todos os scripts:** Todos os scripts no servidor núcleo.

Você pode criar grupos sob o item **Meus scripts** para categorizar mais seus scripts. Para criar um novo script, clique o botão direito no item **Meus scripts** ou em um grupo que você criou e clique no tipo de script que você quiser criar.

A terminar de criar um script, você pode clicar em Agendar no menu de atalho do script. Essa ação abre a janela **Tarefas agendadas** (**Ferramentas > Distribuição > Tarefas armazenadas**) onde você pode especificar os dispositivos onde a tarefa deve ser executada e o horário em que elas devem ser realizadas. Consulte a próxima seção para ver mais informações sobre o agendamento de tarefas.

Devido aos recursos específicos suportados pelo console do Windows, os scripts nele baseados não devem ser editados no Web console.

Agendar uma tarefa

A janela **Tarefas agendadas** exibe o status das tarefas agendadas e se as tarefas foram concluídas com êxito ou não. O serviço de planejador possui dois meios de se comunicar com os dispositivos:

- Através do agente LANDesk padrão (já deve estar instalado nos dispositivos).
- Por meio de uma conta de sistema em nível de domínio. A conta escolhida deve ter o login como privilégio de serviço. Para obter mais informações sobre a configuração da conta do Agendador, consulte a "Configuração do serviço do Agendador" na página 85.

O console inclui scripts que você pode agendar para executar tarefas de manutenção de rotina, tais como a execução de varreduras de inventário nos dispositivos selecionados. Você pode agendar esses scripts em **Ferramentas > Distribuição > Gerenciar scripts > Todos os outros scripts**.

Antes de poder agendar tarefas para um dispositivo, o agente LANDesk padrão deverá estar instalado no dispositivo e o dispositivo deverá estar no banco de dados do inventário.

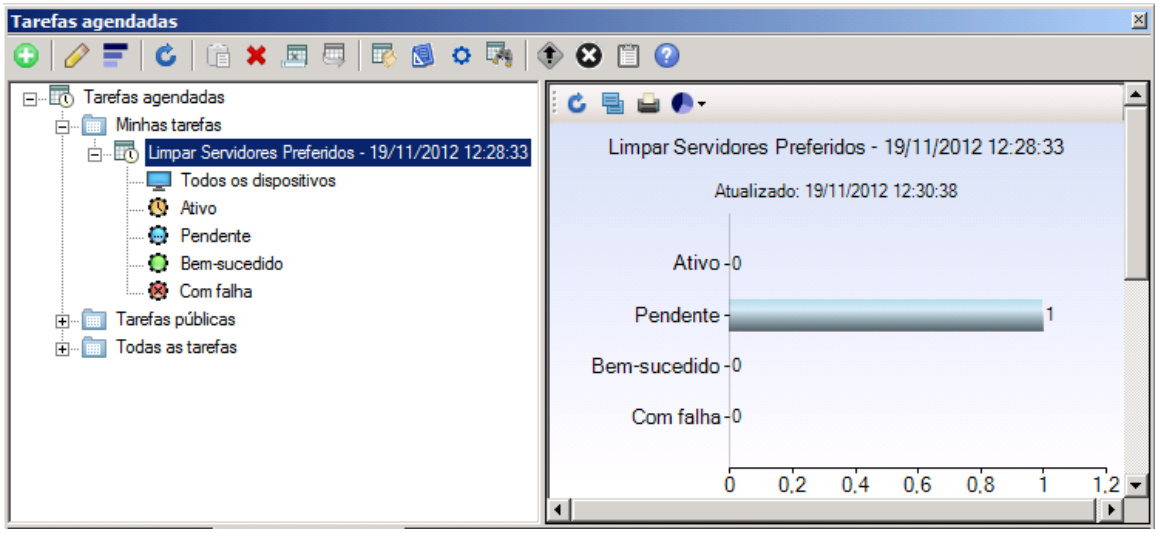
Para agendar uma tarefa

1. Na janela Tarefas agendadas, clique em um dos seguintes botões da barra de ferramentas: **Agendar script personalizado, formulários de dados personalizados, Configuração de agente** ou **Agendar varredura de inventário**.
2. Digite as informações necessárias para o tipo de tarefa que você selecionou.
3. Clique no botão **Agendar**. Aparece a janela **Tarefas agendadas** e adiciona o script a ela, onde torna-se uma tarefa.
4. Na tela de rede, selecione os dispositivos que quiser que sejam alvos de tarefa e arraste-os para a tarefa na janela **Tarefas agendadas**.
5. Na janela **Tarefas agendadas**, no menu de atalho da tarefa, clique em **Propriedades**.
6. Na página **Agendar tarefa**, defina o horário de início da tarefa e clique em **Salvar**.

Você pode adicionar mais dispositivos à tarefa arrastando-as da tela de rede e soltando-as na tarefa que quiser na janela **Tarefas agendadas**.

Usar a janela Tarefas agendadas

Use a janela **Tarefas agendadas** para configurar e agendar scripts que você tenha criado. Agende itens para distribuição uma única vez, ou agende uma tarefa recorrente, por exemplo, uma tarefa de script, para procurar regularmente dispositivos não gerenciados.



A janela **Tarefas agendadas** é dividida em dois painéis. O painel da esquerda mostra a árvore de tarefas e as tarefas, e o da direita mostra informações específicas sobre o que você tiver selecionado na árvore.

Painel esquerdo

O painel esquerdo mostra os seguintes grupos de tarefas:

- **Minhas tarefas:** As tarefas que você agendou. Somente você e os usuários administrativos Management Suite podem ver essas tarefas.
- **Tarefas públicas:** As tarefas que os usuários com direito "Editar público" marcaram público.
- **Todas as tarefas:** As suas tarefas e as tarefas marcadas como comuns.

Você pode arrastar scripts para o painel esquerdo da janela **Tarefas agendadas**. Quando o script estiver no painel esquerdo, você poderá configurar alvos para ele arrastando dispositivos, consultas ou grupos para o painel direito.

Tasks also have a right-click menu that you can use. The right-click Start now menu option has these choices:

- **Todos:** Runs the task on all targeted devices.
- **Dispositivos que não tiveram êxito:** Runs the task only on targeted devices that tried to complete the task but weren't successful.
- **Dispositivos que não tentaram executar a tarefa:** Runs the task only on targeted devices that didn't try to run the task, such as devices that were powered off or not connected to the network.
- **Aguardando ou atualmente trabalhando:** Runs the task on devices that are in a waiting or currently working state. This is useful when devices are stuck in one of these task states and you want to try the task on them again.

Cancelar uma tarefa

Você pode cancelar tarefas em espera ou tarefas ativas. A maneira de cancelar uma tarefa depende do tipo de tarefa, conforme descrito abaixo:

- **Tarefas de distribuição de software:** Use o botão cancelar na barra de ferramentas. Esse botão da barra de ferramentas só está disponível para tarefas de distribuição de software.

- **Scripts personalizados:** No menu de atalho do script que quer cancelar, clique em **Status atual**. O diálogo **Status da tarefa** contém os botões **Descontinuar tarefa** e **Cancelar tarefa**. Clique no botão que desejar.
- **Tarefas em espera:** No menu de atalho da tarefa que quer cancelar, clique em **Propriedades**. Na página **Agendar tarefa**, clique em **Deixar não agendada**.

Atribuir alvos a uma tarefa

Assim que tiver adicionado um script à janela **Tarefas adicionadas** você pode atribuir alvos a ele. Arraste alvos da tela de rede para a tarefa que quiser na janela **Tarefas agendadas**. Os alvos podem incluir dispositivos individuais, grupos de dispositivos, objetos LDAP, consultas LDAP e consultas de inventário. Consultas e grupos são poderosas opções que lhe permitem ter uma lista dinâmica de dispositivos que podem ser modificados para tarefas recorrentes. Por exemplo, à medida que muda a lista de alvos de dispositivos de uma consulta, qualquer tarefa que utilize essa consulta terá como alvo automaticamente os novos dispositivos.

Se um dispositivo é selecionado como alvo mais de uma vez, como quando duas consultas alvo tiverem resultados sobrepostos, o servidor núcleo detecta a duplicação e não executará repetidas vezes para o mesmo dispositivo.

Nas consultas para tarefas alvo, a consulta não é executada até a tarefa iniciar. O diálogo **Propriedades de tarefas agendadas** não mostrará os dispositivos alvo até depois de a tarefa ser iniciada.

Aplicação de escopo a tarefas

Para tarefas agendadas, usuários múltiplos Management Suite podem adicionar alvos a uma tarefa. Entretanto, na janela **Tarefas agendadas**, cada usuário Management Suite verá somente alvos dentro de seu escopo. Se dois usuários Management Suite com escopos que não se sobrepõem, adicionam 20 alvos a uma tarefa, cada usuário Management Suite exibirá somente os 20 alvos que ele adicionou, mas a tarefa será executada em todos os 40 alvos.

Seleção de alvos para sua tarefa

Cada tarefa que você cria precisa de um conjunto de alvos onde a tarefa será executada. As tarefas podem ter dois tipos de alvos, estático e dinâmico.

- **Alvos estáticos:** uma lista de dispositivos ou usuários específicos que não são alterados a menos que você o faça manualmente. Os alvos estáticos podem ser usuários LDAP do Directory Manager ou de dispositivos da tela de rede do console.
- **Alvos dinâmicos:** uma lista dinâmica de dispositivos que permite às tarefas de distribuição baseada em diretiva verificar periodicamente se existem alterações na lista de alvos. Os alvos dinâmicos incluem resultados de consultas e grupos/contêineres LDAP ou grupos de tela de rede.

Os alvos dinâmicos da diretiva são únicos, e o Management Suite atualiza os resultados dessas consultas periodicamente. Quando novos dispositivos atendem aos critérios da consulta, as tarefas recorrentes que usam essas consultas são aplicadas aos novos dispositivos.

É possível especificar os alvos estáticos da diretiva de acordo com os seguintes procedimentos:

- **Dispositivos da Tela da rede:** um conjunto estático de dispositivos do banco de dados núcleo.
- **Usuários ou dispositivos LDAP:** um conjunto estático de objetos usuário e/ou dispositivo.

É possível especificar os alvos dinâmicos da diretiva de acordo com os seguintes procedimentos:

- **Grupo da Tela da rede:** um conjunto dinâmico de dispositivos do banco de dados núcleo.
- **Grupo/contêiner LDAP:** Um conjunto dinâmico de objetos usuário, computador ou grupo.
- **Consulta do banco de dados:** um conjunto de dispositivos gerado por uma consulta no banco de dados núcleo.
- **Grupo de usuários:** um grupo de usuários selecionados em um diretório compatível com LDAP.
- **Consulta LDAP:** Um conjunto de usuários, dispositivos, ou ambos, gerado por uma consulta em um diretório compatível com LDAP.

Dispositivo-alvo através de um diretório

Para que os dispositivos recebam diretivas direcionadas pelo Active Directory, eles precisam ser configurados para fazer o logon no diretório. Isso significa que eles precisam que todo o software de dispositivo esteja instalado corretamente e que iniciem a sessão no diretório correto para que seu nome, totalmente distinto, coincida com o nome direcionado por meio do Directory Manage.

Para cada dispositivo Windows, deve haver uma conta de computador no controlador de domínio do Active Directory. Isso significa que o computador que estiver sendo usado como dispositivo deve ter feito logon no domínio em que o Active Directory residir. Você não pode simplesmente mapear uma unidade de rede usando o nome de domínio do Windows completamente qualificado. A diretiva não terá efeito dessa maneira.

Para usar o Gerenciador de diretórios para criar uma consulta:

1. Clique em **Ferramentas > Distribuição > Gerenciador de diretórios**.
2. Clique no botão da barra de ferramentas **Gerenciar diretório**.
3. Digite o URL do diretório e as informações de autenticação e clique em **OK**.
4. Clique no botão da barra de ferramentas **Nova consulta**.
5. Crie a sua consulta. Para obter mais informações, consulte "Consultas LDAP" na página 184.

O que você vê quando as tarefas são executadas

A janela **Tarefas agendadas** sempre mostra o status dos trabalhos. Se você estiver agendando configurações de dispositivos ou distribuições de SO, a caixa de diálogo **Utilitário de configuração do cliente** também aparecerá. À medida que o serviço agendador continua pela lista de alvos, você verá uma lista com os dispositivos a configurar, dispositivos sendo configurados e listas de dispositivos concluídos. Para obter mais informações, consulte "Sobre a caixa de diálogo Utilitário de configuração do cliente" na página 137.

Se você estiver atualizando distribuições por Multidifusão dirigida, aparecerá a janela de **Status da distribuição de software por multidifusão**. Essa janela mostra o status da multidifusão. Para obter mais informações, consulte "Sobre a janela Status de distribuição de software por multidifusão" na página 299.

Se estiver agendando scripts personalizados, você verá a janela **Processamento de tarefas personalizadas**, exibindo os dispositivos alvo agendados, em andamento e concluídos, além de um status do script linha por linha à medida que é executado.

Monitoramento do status da tarefa

Quando a tarefa inicia o processo, os dispositivos alvo passam por vários status da tarefa. Você pode monitorar o estado da tarefa dos dispositivos alvo clicando na tarefa ativa na janela **Tarefas agendadas**. Os dispositivos estarão em uma das seguintes categorias:

- **Todos os dispositivos:** Todos os alvos para a tarefa.
- **Ativo:** Alvos que estão sendo processados atualmente.
- **Pendente:** Alvos que ainda não foram processados.
- **Bem sucedido:** Alvos que terminaram a tarefa com sucesso.
- **Com falha:** Alvos onde a tarefa falhou.

Esses são os estados do dispositivo e a categoria que onde eles são visíveis:

- **Aguardando:** Pronto para processar a tarefa.; categoria **(pendente)**
- **Ativo:** Processando a tarefa atual; categoria **(ativa)**
- **Terminado:** Tarefas processadas com sucesso; categoria **(com sucesso)**
- **Ocupado:** O dispositivo já está processando uma tarefa diferente e não conseguiu processar a tarefa atual; categoria **(com falha)**.
- **Com falha:** Não terminou de processar a tarefa pela mesmo motivo; categoria **(com falha)**.
- **Desativado:** O dispositivo estava desativado ou não acessível; categoria **(com falha)**.
- **Cancelado:** O usuário cancelou a tarefa; categoria **(com falha)**.

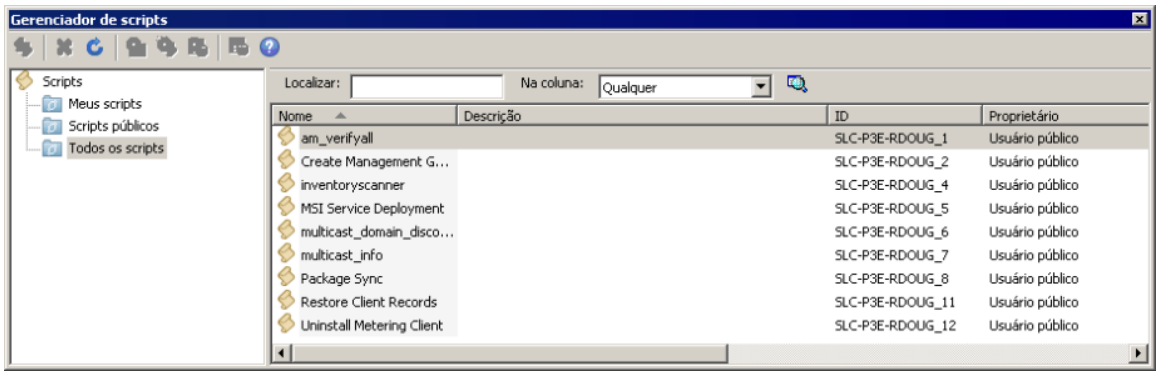
Como ver logs de tarefas

Se um dispositivo falhar no processamento da tarefa, a janela **Tarefas agendadas** armazena o log da tarefa. Os logs disponíveis aparecem na coluna **Arquivo de log** próxima a um disponível. No arquivo de log você pode ver o comando da tarefa que falhou.

Uso de scripts padrão

O Management Suite é vendido com um conjunto de scripts padrão os quais são descritos abaixo. Você pode usá-los para ajudar a realizar algumas tarefas Management Suite. Esses scripts estão disponíveis na árvore **Todos os outros scripts** na janela **Gerenciar scripts** (**Ferramentas > Distribuição > Gerenciar scripts**):

- **am_verifyall:** Verifica todos os pacotes instalados por meio de diretivas nos clientes.
- **Criar certificado de cliente do Management Gateway:** Cria um certificado de segurança para que um dispositivo possa usar um Management Gateway.
- **inventoryscanner:** Executa o analisador de inventário nos dispositivos selecionados.
- **multicast_domain_discovery:** Executa uma descoberta do representante de domínio de Multidifusão dirigida.
- **multicast_info:** Executa um script de solução de problemas que mostra quais informações a janela Tarefas agendadas passará para uma Multidifusão dirigida, incluindo informações de sub-rede e endereços IP do dispositivo alvo. Cria um arquivo denominado c:\mcinfo.txt.
- **Sicronização do Pacote:** Executa uma verificação de diretiva para ver se qualquer das novas diretivas precisa ser aplicada ou tornada disponível.
- **Restaurar os registros do cliente:** Executa o analisador de inventário em dispositivos selecionados, mas o analisador reporta ao núcleo de onde o dispositivo foi configurado. Se tiver que reconfigurar o banco de dados, esta tarefa ajuda a adicionar dispositivos de volta ao banco de dados núcleo correto em ambiente com vários núcleos.
- **Desinstalação do cliente de monitoração:** Remove o agente de monitoração de software dos computadores de destino. Esse agente era usado no Management Suite antes da versão 8.



Opções da largura de banda de tarefas

Ao configurar comandos do Agendador local, você pode especificar os critérios mínimos de largura de banda necessários para a execução da tarefa. O teste de largura de banda consiste no tráfego da rede para o dispositivo que você especificar. Quando for o momento de execução da tarefa, cada dispositivo que estiver executando a tarefa do planejador local enviará uma pequena quantidade de tráfego de rede de ICMP para o dispositivo que você especificar e avaliará o desempenho. Se o dispositivo alvo de teste não estiver disponível, a tarefa não será executada.

Podem ser selecionadas as seguintes opções de largura de banda:

- **RAS:** A tarefa é executada se a conexão de rede do dispositivo ao dispositivo alvo possuir pelo menos RAS ou velocidade de dial-up, conforme detectado pela API de rede. A seleção dessa opção, em geral, significa que a tarefa sempre será executada se o dispositivo tiver algum tipo de conexão de rede.
- **WAN:** A tarefa será executada se a conexão do dispositivo ao dispositivo alvo possuir pelo menos velocidade de WAN. Velocidade WAN é definida como uma conexão não RAS que é mais lenta que o limite da LAN.
- **LAN:** A tarefa será executada se a conexão do dispositivo ao dispositivo alvo exceder o parâmetro de velocidade de LAN. Por padrão, a velocidade é definida como qualquer valor acima de 262.144 bps. Você pode definir o limite da LAN na configuração do agente (página **Ferramentas > Configuração > Agente > Configuração, Detecção de largura de banda**). As mudanças não terão efeito até você distribuir a configuração atualizada aos dispositivos.

Usar o núcleo de rollup para agendar uma tarefa globalmente

Se você tem um núcleo de rollup em seu ambiente LANDesk, as tarefas que você criar nele são agendadas globalmente e podem ter alvos de vários núcleos filhos. Quando você criar uma tarefa no núcleo rollup e agendá-la, ele checa a lista de alvos para ver quais alvos pertencem a quais servidores núcleo filhos. O núcleo rollup então envia a cada servidor núcleo filho a tarefa e sua parte exclusiva da lista geral de alvos. Cada servidor núcleo filho executa a tarefa no fundo e faz um relatório do status da tarefa ao núcleo rollup.

Se o servidor núcleo filho tiver alvos, mas não tiver certificado do núcleo rollup, o qual é necessário para o núcleo filho processar tarefas agendadas globalmente, o núcleo rollup executa ele mesmo a tarefa nesses alvos.

As tarefas agendadas globalmente e o status de tarefa não aparecem na janela **Tarefas agendadas** do núcleo filho. O lugar mais fácil para ver essas informações é nos detalhes da tarefa no núcleo rollup. Se quiser ver o status da tarefa delegada em um núcleo filho que a está processando, use o relatório Tarefas delegadas.

NOTA: As tarefas agendadas de um núcleo de rollup 9.0, incluindo tarefas relacionadas a segurança nos núcleos 8.7 e 8.8.

Para ver o status da tarefa delegada em um núcleo filho

1. No núcleo filho, clique em **Ferramentas > Relatórios / Monitoração > Relatórios**.
2. Na janela relatórios, clique em **Relaltórios > Management Suite > Status da tarefa**.
3. Clique duas vezes no relatório **Tarefas delegadas** e digite o intervalo de datas que deseja.
4. Clique em **OK** para ver o relatório.

Para reduzir o tráfego na rede, o status da tarefa delegada não é reportado em tempo real ao núcleo rollup. Em vez disso, como padrão, o status da tarefa é atualizado a cada dois minutos. Faça o seguinte para mudar este intervalo.

Para mudar o intervalo de verificação do status da tarefa

1. No núcleo de rollup, clique em **Iniciar > Programas > LANDesk > LANDesk Configurar serviços**.
2. Na guia **Agendador**, clique em **Avançado**.
3. Clique em **Verificação de status da tarefa delegada** e clique em **Editar**.
4. Digite os segundos que deseja para o intervalo entre verificações do status no agendador e clique em **OK**. O padrão é 120 segundos.
5. Na guia **Agendador**, **Reinicie** o serviço do agendador no núcleo rollup.

Ajuda das tarefas agendadas

Sobre a caixa de diálogo Agendar tarefa

Acesse esta caixa de diálogo da janela **Tarefas agendadas** (**Ferramentas > Distribuição > Tarefas agendadas**). Na janela **Tarefas agendadas**, clique no botão da barra de ferramentas **Criar tarefa de distribuição de software** ou do menu de atalho da tarefa que quiser configurar, clique em **Propriedades**.

Use esta caixa de diálogo para definir o horário de início para a tarefa e torná-la recorrente ou não e com que freqüência. Esta caixa de diálogo também mostra as tarefas alvo. Dependendo do tipo de tarefa que estiver agendando, você pode também ver opções para métodos de distribuição e pacotes de distribuição.

Sobre cópia de tarefas

É também possível criar grupos para a categorização das suas tarefas comuns. Outros usuários só verão grupos se o escopo do RBA permitir que vejam a tarefa naquele grupo. Se você tentar excluir um grupo com tarefas, não poderá excluí-las se não tiver permissão de ver o respectivo escopo.

Sobre a página Descrição

Essa página permite escolher outro proprietário para a tarefa e faz um resumo das escolhas que você fez na caixa de diálogo Tarefas agendadas. Se quiser modificar qualquer de suas escolhas, clique em **Mudar** ao lado da escolha. Se quiser que a tarefa apareça no grupo **Tarefas comuns** da janela **Tarefas agendadas** em vez do grupo **Minhas tarefas**, clique em **Mostrar tarefas comuns**.

Sobre a página Pacote de distribuição

Use essa página para selecionar o pacote de distribuição que deseja distribuir. Ao selecionar um **Tipo de pacote** a lista **Pacote de distribuição**, mostra os pacotes daquele tipo que você pode distribuir. Os pacotes na lista correspondem aos pacotes que você pode ver sob aquele tipo na janela **Pacotes de distribuição** relativos ao usuário atual e ao usuário público. Clique no **Pacote de distribuição** desejado.

As tarefas de distribuição de software baseadas em envio podem conter um pacote preliminar e um pacote final. Ao usar pacotes múltiplos, os pacotes são instalados em ordem, um por vez. O pacote anterior deve retornar um status bem sucedido de tarefa antes do próximo pacote começar a instalar. Para ver mais informações, consulte "Uso de vários pacotes de distribuição em uma tarefa" na página 269".

Sobre a página Método de entrega

Use essa página para selecionar o método de distribuição para usar para o pacote que estiver distribuindo. Ao selecionar um **Tipo de entrega** a lista **Métodos de entrega** mostra os métodos de entrega do tipo que você pode usar. Os métodos de entrega na lista correspondem aos métodos de entrega que você pode ver na janela **Métodos de entrega** relativos ao usuário atual e ao usuário público. Clique no **Método de entrega** desejado.

Sobre a página Dispositivos alvo

Use esta página para ver dispositivos alvo para a tarefa que você está configurando. Você pode adicionar alvos nesta página. Também é possível adicionar alvos mais tarde arrastando-os e soltando-os na tarefa na janela **Tarefas agendadas**. Dispositivos dirigidos podem estar dentro das seguinte categorias:

- Dispositivos alvo
- Objetos LDAP alvo
- Consultas alvo
- Consultas LDAP alvo
- Grupos de dispositivos alvo

Você pode também selecionar a opção **Ativar Dispositivos** nessa página. Essa opção desperta um computador suspenso para a tarefa selecionada com o uso de Wake On LAN. Quando a tarefa é concluída, o computador desliga novamente. Esse recurso funciona apenas em computadores com versões da BIOS que suportam a tecnologia Wake on LAN. A seleção dessa opção tornará as tarefas mais longas, pois a tarefa aguarda os dispositivos que acabaram de despertar para inicialização. Não selecione essa opção para pacotes de distribuição de instalação por recepção.

Sobre a página de Mensagens personalizadas

Use esta página se você quer configurar uma mensagem personalizada que apareça quando a tarefa é executada. A origem da página HTML para as páginas de atraso está no servidor núcleo da pasta LDLogon\html\.

- **Não usar mensagem personalizada para esta tarefa:** Nenhuma mensagem personalizada é exibida. Este é o padrão.
- **Uso das páginas personalizadas HTML:** Usa as páginas HTML na pasta LDLogon\html\ do servidor núcleo.
- **Incluir uma mensagem personalizada na caixa de diálogo de intervalos:** Acrescenta texto que você digita na caixa de diálogo de intervalos (inclusive formatação HTML), substituindo o texto padrão que é normalmente inserido. A caixa de diálogo ainda pode mostrar os botões **Aguardar**, **Cancelar** e **Instalar agora** com texto descrevendo cada ação.

Sobre a página Agendar tarefa

Use esta página para configurar quando a tarefa é executada e quantas tentativas devem ser feitas:

- **Deixar sem agendar:** Adiciona a tarefa à janela Tarefas agendadas, mas não agenda a tarefa. Use essa opção se quiser preservar uma configuração de tarefa, mas não quiser que ela seja executada.
- **Iniciar agora:** Inicia a tarefa assim que a caixa de diálogo for fechada. Pode haver um atraso de até um minuto antes de a tarefa ser realmente iniciada.
- **Iniciar mais tarde:** Inicia a tarefa na hora e data especificadas.
- **Data e hora:** Executa a tarefa na data selecionada. Digite a data usando o formato DD/MM/AA ou clique na lista de datas para selecionar a data de um calendário.
- **Repetir a cada:** Agenda a tarefa a ser repetida periodicamente. Selecione o Dia, Semana ou Mês na lista para escolher com que freqüência a tarefa será repetida. Ela será repetida na hora definida acima.
- **Distribuir pacotes nesta tarefa mesmo se elas foram distribuídas anteriormente:** Reinstala os pacotes nesta tarefa se os pacotes foram já instalados.
- **Agendar estes dispositivos:** Na primeira vez que uma tarefa for executada, deixe o padrão como **Agendar estes dispositivos**. Para execuções subseqüentes, escolha entre **Todos**, **Dispositivos que não tiveram êxito** ou **Dispositivos que não tentaram executar a tarefa**. Essas opções são explicadas abaixo em maiores detalhes.

Ao reagendar uma tarefa, você pode limitar o número de dispositivos nos quais a tarefa é executada. Você pode desejar utilizar esta opção se a tarefa falhou em um grande número de dispositivos, e, por exemplo, não há a expectativa de mudança de estado dos dispositivos que falharam. Limitar a tarefa deste modo ajudaria a tarefa a ser completada mais rapidamente por que o agendador não continuaria a tentar executar a tarefa em dispositivos que não a processaram. Você pode decidir executar tarefas em dispositivos nos seguintes estados:

- **Aguardando ou atualmente trabalhando:** Este é o padrão e deve ser usado na primeira vez que a tarefa é executada. Se você estiver executando a tarefa novamente, esta opção seleciona os dispositivos alvo nos quais a tarefa foi executada com êxito na primeira execução .
- **Todos:** Selecione esta opção se desejar que a tarefa seja executada em todos os dispositivos, independentemente do estado do dispositivo. Considere o uso desta opção se você tiver uma tarefa, especialmente se for repetitiva, que precisa ser executada no maior número de dispositivos possível.
- **Dispositivos com falha:** Selecione esta opção somente se desejar que a tarefa seja executada em todos os dispositivos que não completaram a tarefa da primeira vez. Isto exclui os dispositivos com o estado **Bem-sucedido**. A tarefa será executada em dispositivos em todos os outros estados, inclusive **Aguardando** ou **Ativo**. Considere o uso desta opção se precisar executar a tarefa no maior número possível de dispositivos que falharam, mas só é necessário que a tarefa seja completada com êxito uma vez em cada dispositivo.
- **Dispositivos que não tentaram executar a a tarefa:** Selecione esta opção somente se desejar que a tarefa seja executada em dispositivos que não completaram a tarefa e nos quais não houve falha da tarefa. Isto exclui dispositivos que estavam nos estados **Desligado**, **Ocupado**, **Com falha** ou **Cancelado**. Considere o uso desta opção se houver um grande número de dispositivos alvo nos quais a tarefa falhou, e que não são importantes como alvos.

Sobre a página Script personalizado

Use esta página após agendar um script personalizado e você quer ver qual será o conteúdo do script personalizado. Você não pode editar o conteúdo do script personalizado nesta página.

Sobre a caixa de diálogo Agenda

Vários agentes do Management Suite têm recursos que podem ser agendados com o uso do agente de agendamento local que é instalado nos dispositivos gerenciados. Use essa caixa de diálogo para configurar esse agendamento.

Você também pode usar o Agendador local para agendar suas próprias tarefas de forma a executá-las periodicamente nos dispositivos. Ao ser criado o script do agendador local ou se o agendamento for personalizado para um dispositivo, você pode distribuí-lo aos dispositivos através da janela **Tarefas agendadas**.

Para configurar uma tarefa de agendador local, na janela **Scripts gerenciados** (**Ferramentas > Distribuição > Scripts gerenciados**), no menu de atalho **Meus scripts**, clique em **Novo script de agendador local**.

Todos os critérios na configuração desta caixa de diálogo devem ser satisfeitos antes da tarefa executar. Por exemplo, se você configurar um horário que se repetir todos os dias entre as 8h e 9h com o **Estado do computador** em **Desktop deve estar bloqueado**, a tarefa será executada somente se for entre 8h e 9h e se o dispositivo estiver bloqueado.

Essas opções estão disponíveis na caixa de diálogo **Agenda**:

Seção de eventos

A seção de eventos é escurecida a menos que estiver configurando um script do agendador local da ferramenta **Gerenciar scripts**.

- **Executar quando o usuário fizer login:** Selecione esta opção para executar a tarefa quando um usuário fizer login. Quando um usuário fizer login, o agendador local executará a tarefa diretamente.
- **Executar quando o endereço IP do computador mudar:** Selecione esta opção se quiser que a tarefa seja executada se o endereço IP do dispositivo mudar ou é renovada através de DHCP. Por exemplo, use esta opção para disparar uma varredura de inventário quando o endereço IP mudar, para manter o endereço IP sincronizado no banco de dados do Management Suite.

Seção horário

Use esta seção para configurar os horários de execução das tarefas. Se você iniciou esta caixa de diálogo da ferramenta de configuração de agentes, você pode especificar um atraso aleatório da página de configuração de agentes. O intervalo de atraso aleatório que você especificar é um intervalo de tempo durante o qual a tarefa executará. Por exemplo, se você tiver um número grande de usuários que fazem login ao mesmo tempo, este atraso permite que tarefas que executam durante o login não executem ao mesmo tempo, assumindo que o intervalo de atraso é suficientemente longo. O atraso padrão é uma hora.

- **Iniciar:** Clique esta opção para exibir um calendário onde pode selecionar o dia que você quer que a tarefa inicie. Uma vez escolhido o dia, você pode também digitar uma hora do dia. Estas opções são definidas à data e hora atual.
- **Repetir depois de:** Se desejar a tarefa recorrer, clique na caixa de listagem e selecione **minutos**, **horas**, ou **dias**. Em seguida na primeira caixa digite o tempo de duração que deseja para o intervalo selecionado .
- **Intervalo de tempo:** Se desejar que a tarefa execute em horas específicas, selecione as horas de início e final. As horas estão no formato de 24 horas
- **Semanalmente entre:** Se desejar que a tarefa execute em dias específicos da semana, selecione os dias de início e final.

- **Mensalmente entre:** Se desejar que a tarefa execute em datas específicas do mês, selecione as datas de início e final.

Seção de filtros de execução

Ao configurar comandos do agendador local, você pode especificar os critérios mínimos de largura de banda necessários para a execução da tarefa. O teste de largura de banda consiste no tráfego da rede para o dispositivo que você especificar. Quando for o momento de execução da tarefa, cada dispositivo que estiver executando a tarefa do Agendador local enviará uma pequena quantidade de tráfego de rede de ICMP para o dispositivo que você especificar e avaliará o desempenho. Se o dispositivo alvo de teste não estiver disponível, a tarefa não será executada.

Ao especificar o critério da largura de banda para dispositivos que possam estar conectando ao núcleo através do LANDesk Management Gateway, você deve colocar o endereço IP do Management Gateway no campo **para**. Isto permite que o teste da largura de banda conclua e que a tarefa execute.

Podem ser selecionadas estas opções de **Largura de banda mínima**:

- **RAS:** A tarefa é executada se a conexão de rede do dispositivo ao dispositivo alvo possuir pelo menos RAS ou velocidade de dial-up, conforme detectado pela API de rede. A seleção dessa opção, em geral, significa que a tarefa sempre será executada se o dispositivo tiver algum tipo de conexão de rede.
- **WAN:** A tarefa será executada se a conexão do dispositivo ao dispositivo alvo possuir pelo menos velocidade de WAN. Velocidade WAN é definida como uma conexão não RAS que é mais lenta que o limite da LAN.
- **LAN:** A tarefa será executada se a conexão do dispositivo ao dispositivo alvo exceder o parâmetro de velocidade de LAN. Por padrão, a velocidade é definida como qualquer valor acima de 262.144 bps. Você pode definir o limite da LAN na configuração do agente (página **Ferramentas > Configuração > Agente > Configuração, Detecção de largura de banda**). As mudanças não terão efeito até você distribuir a configuração atualizada aos dispositivos.

A seção de filtros de execução tem estas opções:

- **Largura de banda mínima:** Se você quer que os critérios da execução da tarefa incluam a largura de banda disponível, selecione a largura de banda mínima que deseja e digite o nome do dispositivo ou o endereço IP que será o alvo para o teste da largura de banda entre o alvo e o dispositivo.
- **Estado da máquina:** Se você quiser que os critérios de execução da tarefa inclua o estado de computador, selecione um desses estados. **Proteção de tela ou desktop bloqueado**, **Desktop deve estar bloqueado**, **Máquina deve estar inativa**, **Usuário deve estar conectado**, ou **Usuário deve estar desconectado**. Os critérios para o estado **Máquina deve estar inativa** são: o SO está bloqueado, a proteção de tela está ativa ou o usuário está desconectado.

Outras opções:

- **Atraso aleatório adicional uma vez que os outros filtros forem aprovados:** Se desejar um atraso aleatório adicional, use esta opção. Se selecionar um atraso aleatório que ultrapassa os limites de tempo configurados para a tarefa, a tarefa pode não executar se o valor aleatório colocar a tarefa fora dos limites de tempo configurados.
- **Atrasar até:** Selecione o atraso aleatório adicional que desejar.
- **E pelo menos:** Se desejar que a tarefa aguarde pelo menos um número específico de minutos antes de executar, selecione esta opção. Por exemplo, se estiver agendando uma varredura de inventário, você pode digitar 5 aqui para o computador ter tempo de concluir a inicialização antes da varredura iniciar, melhorando assim a resposta do computador para o usuário.

- **Comando:** Digite o programa a ser executado localmente. Inclua o caminho completo do programa ou verifique se o programa está numa pasta dentro do caminho do dispositivo. Esse caminho deve ser o mesmo em todos os dispositivos aos quais você distribuir este script.
- **Parâmetros:** Digite qualquer parâmetro da linha de comandos que você quiser passar ao programa.

Agendador local

Uso do agendador local

O agendador local é um serviço executado em dispositivos. Ele é parte do agente de base comum e você pode instalá-lo através da configuração do dispositivo. Em geral, o agendador local cuida das tarefas do como, por exemplo, execução do analisador de inventário periodicamente. Outras tarefas agendas como, distribuições de software ou de SO, são executadas pelo servidor núcleo em vez do agendador local. Você pode usar o planejador local para agendar suas próprias tarefas de forma a executá-las periodicamente nos dispositivos. Ao ser criado o script do planejador local, você pode distribuí-lo aos dispositivos através da janela **Tarefas agendadas**.

O planejador local atribui a cada tarefa um número de ID. Os scripts do agendador local têm uma faixa de IDs diferente dos scripts do agendador local padrão utilizado pelo Management Suite. Como padrão, você pode ter somente um script de agendador personalizado ativo em cada dispositivo. Se você criar um novo script e distribuí-lo aos dispositivos, ele substituirá o script antigo (qualquer script na faixa de IDs do planejador local personalizado) sem afetar os scripts de planejador local padrão como a agenda de análise de inventário local.

Instalar o serviço agendador local em um dispositivo não gerenciado

O serviço Agendador local LANDesk pode ser instalado em um dispositivo não gerenciado. Somente são requeridos dois arquivos para o funcionamento do agendador local:

- LocalSch.exe
- LTapi.dll

Para instalar o serviço Agendador local LANDesk em um servidor não gerenciado ou estação de trabalho, siga as etapas abaixo.

1. Criar essa pasta.

```
%ProgramFiles%\LANDesk\LDClient
```

2. Copie LocalSch.exe e LTapi.dll para esta pasta.
3. Clique em **Iniciar > Executar** e digite o seguinte comando.

```
"%ProgramFiles%\LANDesk\LDClient\localsch.exe" /i
```

Remoção do serviço Agendador local

Para desinstalar o serviço Agendador local LANDesk, siga as seguintes etapas abaixo.

1. Clique em Iniciar > Executar e digite o seguinte comando.

```
"%ProgramFiles%\LANDesk\LDClient\localsch.exe" /r
```

2. Exclua os arquivos e pastas.

Adição de uma tarefa com o LocalSch.exe

O resto dos parâmetros da linha de comando são usados para adicionar uma tarefa local. Ao adicionar uma tarefa local, você deve especificar o executável usando o parâmetro /exe. Se o usuário ou processo executando a linha de comando não tem direitos de administrador, a tarefa não será agendada. Se o usuário atual não tem privilégios de administrador, a tarefa não será criada.

Além das opções da linha de comando descritas abaixo, a opção /taskid pode ser usada para especificar a tarefa.

/exe=<executable> - Aplicativo agendado

Especifica o aplicativo que será iniciado quando a hora agendada ocorrer. Se este parâmetro não é fornecido, a tarefa local não será criada.

/cmd=<linha de comando> - Linha de comando do aplicativo

Especifica a linha de comando a ser usada quando o aplicativo agendado for iniciado. Se este parâmetro não for especificado, o aplicativo agendado será iniciado sem parâmetros de linha de comadno.

/start="<data/hora>" – Hora de início

Especifica a hora de início do aplicativo. Se este parâmetro não for especificado, o aplicativo será iniciado logo. Se filtros forem especificados, eles devem ser cumpridos antes do aplicativo iniciar. A hora de início é especificada do horário do sistema local do computador e tem o seguinte formato:

```
/start="06 Nov 2001 17:39:47" /bw=WAN|myserver.domain.com
```

Este formato é uma versão curta do formato usado por HTTP. O mês é especificado sempre usando uma abreviação ASCII de três letras: Jan, Fev, Mar, Abr, Mai, Jun, Jul, Ago, Set, Out, Nov, ou Dez. Se o formato da data for especificado incorretamente, a tarefa não será adicionada.

/freq=xxx – Frequência

Especifica uma freqüência periódica. A freqüência é o número de segundos antes que a tarefa seja executada novamente. Se este parâmetro não for especificado ou for zero, a tarefa será executada somente uma vez.

/user – Filtro usuário

Especifica que um filtro de usuário deve ser criado para a tarefa. Um filtro de usuário impedirá que a tarefa seja executada até que um usuário esteja conectado ao sistema.

/bw=xxx|<host da rede> - Filtro de largura de banda

Especifica a largura de banda necessária para um host de rede específico. A largura de banda pode ser específicada como LAN, WAN, ou RAS. Se outro valor de largura de banda for usado, o planejador local usará a largura de banda RAS padrão. A tarefa não será executada até que o planejador local detectar que o tipo de largura de banda específicado esteja disponível entre o dispositivo e o host de rede especificado.

Por exemplo, o seguinte filtro especificará para não executar a tarefa até que pelo menos uma conectividade WAN esteja disponível no computador meuservidor.domain.com.

```
/bw=WAN|meuservidor.domain.com
```

/tod=<início>|<final> - Filtro da hora do dia

Especifica um filtro da hora do dia. A tarefa não será executada a menos que a hora do dia esteja entre as horas de início e final especificadas. Os valores da hora do dia são especificados como as horas 0 até 23. Por exemplo, o seguinte filtro especificará a execução de uma tarefa entre 7 p.m. e 10 p.m.

```
/tod=19|22
```

/dow=<início>|<final> - Filtro do dia da semana

Especifica um filtro de dia da semana. A tarefa não será executada a menos que o dia da semana esteja entre os dias de início e final especificados. Os valores do dia da semana são especificados como um número inteiro com 0 sendo domingo. Por exemplo, o seguinte filtro especificará a execução de uma tarefa entre domingo e quinta-feira.

```
/dow=0|4
```

/dom=<início>|<final> - Filtro do dia do mês

Especifica um filtro de dia do mês. A tarefa não será executada a menos que o dia do mês esteja entre os dias de início e final especificados. O filtro do dia do mês é especificado usando valores numéricos entre 1 e 31. Por exemplo, o seguinte filtro especificará a execução de uma tarefa entre os dias 16 e 28 do mês.

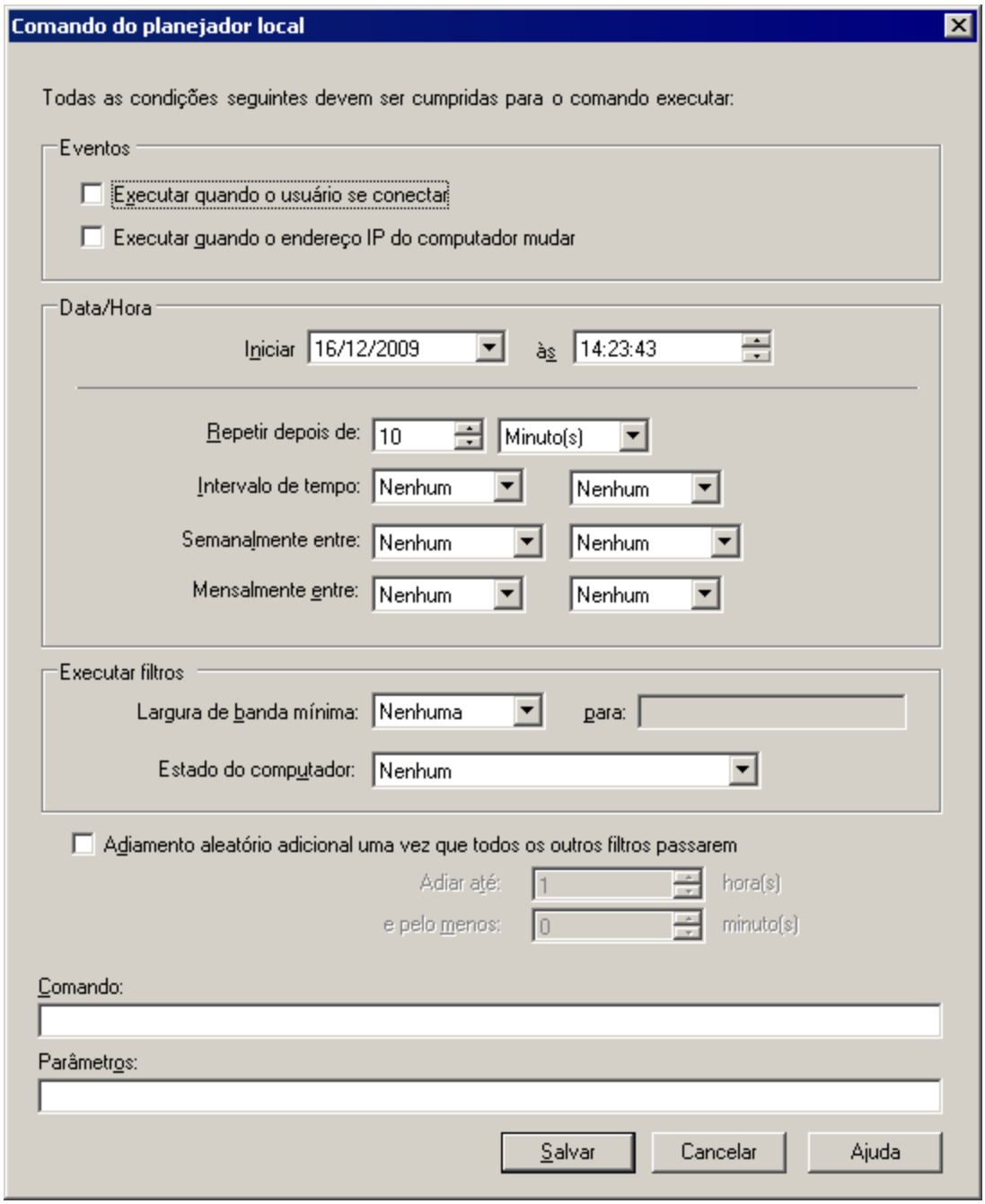
```
/dom=16|28
```

/ipaddr - Filtro de mudança do endereço IP

Especifica que a tarefa deve ser executada cada vez que o endereço IP do computador mudar.

Criar um comando para o agendador local

Ao selecionar as opções de agendamento, não seja tão restrito de forma que o critério da tarefa seja correspondido de forma pouco freqüente, a menos que essa seja sua intenção. Por exemplo, ao configurar uma tarefa, se você selecionar segunda-feira para o dia da semana e 17 para o dia do mês, a tarefa só será executada numa segunda-feira que seja também 17 do mês, o que ocorre com pouca freqüência.


Comando do planejador local
Todas as condições seguintes devem ser cumpridas para o comando executar:
Eventos
Executar quando o usuário se conectar
Executar quando o endereço IP do computador mudar
Data/Hora
Iniciar 16/12/2009 às 14:23:43
Repetir depois de: 10 Minuto(s)
Intervalo de tempo: Nenhum Nenhum
Semanalmente entre: Nenhum Nenhum
Mensalmente entre: Nenhum Nenhum
Executar filtros
Largura de banda mínima: Nenhuma para:
Estado do computador: Nenhum
Adiamento aleatório adicional uma vez que todos os outros filtros passarem
Adiar até: 1 hora(s)
e pelo menos: 0 minuto(s)
Comando:
Parâmetros:
Salvar
Cancelar
Ajuda

Criar um comando para o agendador local

1. Na janela **Scripts gerenciados** (**Ferramentas > Distribuição > Scripts gerenciados**), no menu de atalho Meus scripts, clique em **Novo script de agendador local**.
2. Digite um **Nome de script**.
3. Clique em **Adicionar** para definir as opções do script.
4. Configure as opções do agendador local conforme descrito anteriormente.

5. Clique em **Salvar** para salvar o script.
6. Use a janela **Tarefas agendadas** para distribuir o script que você criou para os dispositivos.

Exclusão de uma tarefa com o LocalSch.exe

O planejador local fornece a habilidade de excluir uma ou mais tarefas. Os seguintes parâmetros são usados ao excluir tarefas.

/del – Excluir tarefa ou tarefas

Exclui a tarefa especificada pelo parâmetro /taskid ou exclui todas as tarefas dentro dos valores máximos e mínimos de /range inclusive. Os IDs da tarefa podem ser determinados olheando as tarefas usando a opção da linha de comando /tasks ou usando uma constante /taskid ao adicionar uma tarefa.

/removetasks – Remover todas as tarefas

Remove todas as tarefas locais atualmente agendadas.

/taskid – Especificando o ID da tarefa

Especifica o ID da tarefa que está sendo excluída. Os IDs da tarefa podem ser determinados olheando as tarefas atualmente agendadas (veja /tasks acima). O ID é especificado como um valor de número inteiro.

/range=<mín>|<máx> – Intervalo de IDs de tarefa

Especifica um valor mínimo e máximo de um intervalo de IDs de tarefa. Ele pode ser usado com o comando /del para remover todas as tarefas com IDs de tarefa dentro do intervalo especificado.

Geralmente ao gerar uma tarefa, um ID é designado aleatoriamente usando o valor da hora atual (time_t) como o do ID de tarefa. Um ID designado aleatoriamente nunca será menor do que 100000. Este parâmetro da linha de comando pode ser usado para especificar o ID da tarefa. Valores de ID de tarefa de 0 -1000 são reservados para uso interno do LANDesk. Valores do ID de tarefa 1001-2000 são reservados para uso da interface do planejador do console de gerenciamento.

Parâmetros de linha de comando de LocalSch.exe

Além de monitorar e executar tarefas locais, o LocalSch.exe pode ser usado para instalar ou remover o serviço, adicionar novas tarefas e exibir todas as tarefas atualmente configuradas.

As seguintes são opções de linha de comando suportadas pelo planejador local.

```
LocalSch.exe [/i] [/r] [/d] [/tasks] [/isinstalled] [/del] [/removetasks]
 [/exe=<executable>] [/cmd=<command line>] [/start="<date/time>"] [/freq=xxx]
 [/user] [/bw=xxx|<server>] [/tod=<begin>|<end>] [/dow=<begin>|<end>]
 [/dom=<begin>|<end>] [/ipaddr] [/taskid=<id>] [/range=<min>|<max>]
```

/i – Instalar serviço

Instala o serviço planejador local no dispositivo Após ser instalado, o planejador local precisará ainda ser iniciado.

/r – Remover serviço

Remove o serviço agendador local do computador. O serviço planejador local deve ser interrompido antes que você remova o serviço.

/d – Executar no modo depurar

Executa o planejador local em modo depurar. Ao executar em modo depurar, o planejador local executa como um processo normal de Windows e não como um serviço ou pseudo serviço. Este modo não resulta em nenhuma saída de duparação adicional.

/isinstalled – Verificar se instalado

Verifica se o serviço planejador local foi instalado no computador local. Este método retornará S_OK, ou zero, se o planejador local foi instalado. Se o planejador local não foi instalado, um valor diferente de zero será retornado.

/tasks – Exibe as tarefas

Este comando mostrará as tarefas atualmente configuradas para stdout mas somente podem ser vistas em uma linha de comando se o parâmetro | more for adicionado.

```
LocalSch.exe /tasks | more
```

Esta saída pode ser redirecionada a um arquivo de texto, por exemplo tasks.txt, usando a seguinte linha de comando:

```
LocalSch.exe /tasks > tasks.txt
```

Análise de caractere do agendador local e a linha de comando

O agendador local usa a análise delimitada por espaço em branco padrão para a linha de comando. Isto significa que se qualquer dos parâmetros contém espaço em branco ele precisa estar encerrado entre aspas. Alguns parâmetros, como /start, sempre contêm espaço em branco e então sempre precisam estar entre aspas. Outros parâmetros, como /exe e /cmd, podem ou não conter espaço em branco e podem ou não precisar estar entre aspas.

O seguinte exemplo mostra uma linha de comando que não precisa estar entre aspas.

```
LocalSch.exe /exe=c:\windows\system32\cmd.exe
```

O seguinte exemplo mostra uma linha de comando que precisa estar entre aspas.

```
LocalSch.exe /exe="%ProgramFiles%\MyProgram\myprog.exe" /cmd="/apm /s /ro"
```

Colocando entre aspas parâmetros que já estão entre aspas

Se os parâmetros que serão passados a /cmd= já estão entre aspas, então três aspas serão necessárias: Um par para colocar a string inteira entre aspas, outro para colocar entre aspas os valores com aspas, e os valores com aspas.

Por exemplo, a seguinte linha de comando mostra um exemplo de parâmetros que precisam ser colocados entre três aspas.

```
LocalSch.exe /exe="%ProgramFiles%\LANDesk\File Replicator\LANDeskFileReplicatorNoUI.exe"
/cmd="""%ProgramFiles%\LANDesk\File Replicator\LDHTTPCopyTaskConfig.xml"" ""%ProgramFiles%\LANDesk\File
Replicator\replicator.log"""
```

No comando acima, os dois parâmetros são caminhos a arquivos. Devido a que os dois caminhos estão no diretório “Arquivos de programa”, eles têm espaço e devem estar entre aspas para serem parâmetros corretos do LANDeskFileReplicatorNoUI.exe. Então, cada parâmetro entre aspas estará rodeado por um segundo par de aspas, e a string inteira estará rodeada por aspas.

Colocando entre aspas operadores de redirecionamento

As aspas devem também rodear qualquer switch que contém um operador de redirecionamento. Os operadores de redirecionamento incluem os seguintes símbolos: <, >, |. O switch /bw usa o caractere | chamado barra. É importante lembrar que o caractere | é usado na linha de comando para direcionar a saída para outro aplicativo. Para impedir que este caractere seja analisado pela linha de comando, ele deve estar entre aspas.

Por exemplo, o seguinte comando usa um parâmetro /bw com um caractere | e precisa estar entre aspas.

```
LocalSch.exe /exe=C:\ldclient\myprogram.exe /cmd="/apm /s /ro" /bw="LAN|server"
```

Controle remoto

Uso da tela de controle remoto

Use a tela do controle remoto para acessar um dispositivo remotamente. Você pode controlar remotamente apenas os dispositivos que têm o agente de controle remoto instalado. Durante uma sessão de controle remoto, o dispositivo remoto tem na verdade dois usuários: você e o usuário final. Você pode fazer remotamente tudo o que o usuário no dispositivo faz.

Se o agente de dispositivo foi configurado para isso (na configuração do agente do dispositivo), você também pode solicitar que o usuário conceda a permissão antes do início de cada nova sessão.

Após a conexão, o ícone de status Remoto aparece no canto superior esquerdo da janela do usuário.

Isto alerta o usuário que sua máquina está sendo controlada remotamente. A qualquer momento o usuário pode clicar com o botão direito no ícone para encerrar a sessão, verificar se ainda está ativa, descobrir quem está controlando remotamente etc.

Você pode fazer muito mais que apenas controlar remotamente um dispositivo a partir da tela. Assim que a tela é conectada ao dispositivo, você pode escolher uma das seguintes tarefas na Barra de ferramentas:

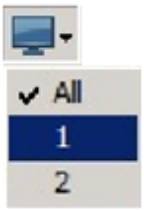
- **Conectar/Desconectar:** Inicia ou termina uma sessão de controle remoto.
- **Iniciar/Interromper exibição:** Exibe ou oculta a tela do dispositivo remoto na tela de exibição do controlador remoto.
- **Bate-papo:** Para bater papo com um usuário em um dispositivo remoto
- **Transferência de arquivos:** Transferência remota de arquivos do seu computador para outro dispositivo. Basicamente, é como se você tivesse mapeado uma unidade de um dispositivo remoto.
- **Reinicialização:** Reinicialização remota de um dispositivo.
- **Desenhar:** Mostra ferramentas de desenho onde poderá usar a tela remota para desenhar.

Você pode realizar múltiplas tarefas na tela em um dispositivo ao mesmo tempo. Quando você ativa a tela de tarefa, a interface da tarefa aparece na janela da tela.

A barra de ferramentas também permite que você controle como o dispositivo remoto é exibido na sua tela. Por exemplo:

- **Tela inteira remota:** Use esta opção para preencher totalmente o monitor local com a tela do dispositivo remoto. Se a resolução da tela remota for maior do que a sua, a Rolagem automática (veja abaixo) pode ser necessária, a menos que você tenha habilitado a opção **Ajustar à tela**.
- **Ajustar à tela:** Já que a janela do visualizador pode ser menor do que a tela do dispositivo remoto, você pode usar esta opção para fazer com que a tela do usuário se ajuste dinamicamente à área visível do seu monitor.

- **Multimonitores:** Se o usuário remoto tem mais de um monitor, este botão será ativado automaticamente, permitindo que você altere rapidamente entre os monitores (até 8) na janela Remota. Você pode minimizar ou redimensionar qualquer dos monitores remotos para facilitar o trabalho na sua janela de controle remoto.

  Se você selecionar a opção **Todos**, todos os monitores serão automaticamente redimensionados para que todos se ajustem a janela do visualizador do controle remoto. Agora você pode selecionar e arrastar para redimensionar os monitores para que fiquem mais fáceis de trabalhar.

A barra de ferramentas também inclui a opção Executar, a qual permite que você busque e execute um programa executável no dispositivo remoto.

Você pode usar o recurso **Rolagem automática** (**Ferramentas> Opções> Mudar configurações > Permitir rolagem automática**) para rolar para cima, para baixo e para os lados. A rolagem automática também rola a janela à medida que o ponteiro do mouse se aproxima da borda da janela.

Você também pode aumentar a área de exibição da janela desativando itens no menu Visualizar, por exemplo, mensagens de conexão, barra de ferramentas ou barra de status.

Se desejar acelerar a exibição ou mudar as configurações da janela do visualizador, use as opções do botão **Otimizar** na barra de ferramentas.

Conetar com dispositivos remotos

Antes de poder realizar qualquer tarefa de controle remoto, é necessário conectar ao dispositivo alvo. É possível conectar diretamente ou através do LANDesk Management Gateway. Somente um visualizador pode se comunicar com um dispositivo por vez, embora você possa abrir várias janelas e controlar dispositivos diferentes ao mesmo tempo. Ao conectar-se a um dispositivo, você pode ver as mensagens e o status da conexão no painel **Mensagens da conexão**, se ele estiver visível. Caso contrário, você pode alternar clicando em **Visualizar > Mensagens de conexão**.

Para conectar-se a um dispositivo

1. Na tela de rede, clique com o botão direito no dispositivo que quiser controlar remotamente, e selecione **Controle remoto, Bate-papo, Transferência de arquivo** ou **execute o controle remoto**.
2. Quando a janela do visualizador for exibida e conectar ao dispositivo remoto, você poderá usar qualquer ferramenta de controle remoto disponível no menu **Ferramentas** da tela de exibição, como bate-papo, transferência de arquivos, reinicialização, inventário ou controle remoto.
3. Para encerrar uma sessão de controle remoto, clique em **Arquivo > Interromper conexão**.

Uso das ferramentas de desenho em dispositivos remotos

Quando estiver vendo um dispositivo remotamente, você pode usar as ferramentas de desenho nele. As ferramentas de desenho podem ajudá-lo a explicar aos usuários o que você está fazendo ou destacar as informações na tela remota para os usuários verem. Quando você usa uma ferramenta de desenho na tela, você e o usuário remoto podem ver o que desenhou. As imagens desenhadas ficam nas duas telas até você clicar no apagador, na paleta da ferramenta de desenho.

Você tem três ferramentas de desenho para usar:

- **Ponteiro:** Use o ponteiro para apontar objetos na tela. Quando você segura o botão esquerdo do mouse a ferramenta ponteiro está ativa e um ponto vermelho aparece sob o ponteiro do mouse que torna fácil aos usuários verem onde o ponteiro está. Quando você solta o botão esquerdo do mouse, o ponto desaparece. Você não pode mudar a cor do ponto e ele não produz um rastro como o lápis.
- **Scribble:** Use a ferramenta scribble para desenhar uma seta, círculos, desenhar a mão livre etc. Não existe limite de formas com a ferramenta scribble.
- **Caixa:** Use a caixa de ferramentas para desenhar um retângulo ao redor de um objeto na tela. Clique onde você quer que um dos cantos do retângulo esteja. Arraste para desenhar um caixa ao redor da área que você quer destacar e solte o botão do mouse.

Você também pode usar as listas suspensas de espessura e cor de linha para mudar a aparência do desenho. As mudanças a esses itens só afetam novos desenhos. Quando você terminar de desenhar, clique no botão de apagar na paleta de desenho ou feche a paleta.

Ajuste das configurações de controle remoto

Use a guia **Mudar configurações** da caixa de diálogo **Ferramentas > Opções** para ajustar as configurações do controle remoto.

- **Permitir rolagem automática:** Permite que a janela do controle remoto role conforme você move o cursor para perto da borda da janela. Quanto mais você se aproximar da borda, mais rápida será a rolagem.
- **Bloquear o teclado e o mouse remotos:** Bloqueia o teclado e o mouse do dispositivo de modo que somente a pessoa que estiver executando a janela do visualizador possa controlar o dispositivo remoto. Observe que as combinações de teclas especiais no Windows, como por exemplo "Ctrl+Alt+Del" ou "Windows Key+L" não estão bloqueadas.
- **Sincronizar clipboards para colar entre os computadores local e remoto:** Sincroniza os teclados entre o dispositivo local e o remoto para você poder colar informações entre os dois dispositivos.
- **Ocultar a tela do computador remoto:** Oculta a tela do dispositivo remoto de modo que somente a pessoa executando o visualizador possa ver a tela no dispositivo remoto.
- **Solicitar sempre para limpar a tela do computador remoto quando iniciar o controle remoto:** Pergunta ao usuário se ele quer deixar em branco sua tela durante o controle remoto. Quando selecionada, o estado da opção **Ocultar a tela do computador remoto** não tem importância.
- **Bloquear o computador remoto quando a sessão terminar:** Quando a sessão termina, essa opção ativa o recurso de bloqueio do sistema operacional. Isto permite que o usuário do controle remoto conclua seu trabalho e protege o sistema do usuário enquanto o usuário está ausente ou até que estejam prontos para continuar uma sessão de controle remoto.

- **Mapeamento automático de teclado:** Essa opção dever ficar selecionada. Ela mapeia novamente o teclado do dispositivo alvo de forma a corresponder ao do administrador. Isso ajuda a garantir que o que o administrador está digitando aparece corretamente no dispositivo alvo. Isso é especialmente útil quando o administrador e os teclados alvo são baseados em alfabetos ou idiomas diferentes.
- **Compatibilidade habilitada para agente antigo (agentes antes da versão 8.5):** A LANDesk modificou a segurança de controle remoto e acrescentou uma nova tela de controle remoto na versão 8.5. Se houver versões do agente de controle remoto na sua rede anteriores à versão 8.5, marque esta opção se quiser permitir que a nova tela se comunique com as versões mais antigas do agente.

Usar nomes alternativos

Dependendo de como você configurou o agente do controle remoto nos dispositivos gerenciados, os usuários em um dispositivo controlado remotamente podem clicar duas vezes no ícone de status do controle remoto na bandeja de sistema do Windows e ver o nome do computador e o nome de usuário do administrador que está o está controlando remotamente. Se não quiser que seu computador ou nome de usuário sejam visíveis a partir dos dispositivos remotos por razões de segurança, é possível especificar um nome de usuário e/ou de computador alternativo que aparece no diálogo do status do controle remoto nos dispositivos remotos.

Para usar nomes alternativos

1. Clique em **Ferramentas > Opções**.
2. Na guia **Alterar as configurações**, selecione **Usar nomes alternativos**
3. Especifique os nomes que quiser que os usuários nos dispositivos remotos vejam.
4. Clique em **OK**.

Uso do driver de espelho

O driver de espelho proporciona muitos benefícios. O benefício principal é a maneira de capturar saída de tela, suportada pela Microsoft, sem precisar de modificação no driver de vídeo. Isso permite um comportamento padrão do driver de espelho do controle remoto, que evita a ocorrência de muitos problemas nos dispositivos.

O outro benefício é o fato de o driver de espelho não requerer de tanto esforço de processamento do dispositivo alvo. Se estiver controlando remotamente dispositivos com processador de 1,5 GHz ou mais lento, o driver de espelho pode proporcionar melhoras significativas de desempenho em conexões de rede mais rápidas. Em conexões de rede mais lentas, o desempenho de controle remoto é limitado mais pela largura de banda que pela utilização do processador.

O agente padrão de controle remoto é sempre instalado em dispositivos. Quando o driver de espelho é instalado no mesmo, o agente padrão e o driver de espelho coexistem. Se quiser, você pode desinstalar o driver de controle remoto e usar apenas o driver de espelho.

Mudança das configurações de tecla de atalho da tela

O visualizador de controle remoto é compatível com as seguintes teclas de atalho (**Ferramentas > Opções > Configurações de teclas de atalho**):

- **Ativar teclas de atalho** (Ctrl + Alt + H): Ativar/desativar a disponibilidade de teclas de atalho. As teclas de atalho estão ativadas por padrão.
- **Fecha a sessão da tela** (Ctrl + Alt + S): Desconectar a sessão de tela atual. A tela do controle remoto permanece aberta.

- **Envia a seqüência Ctrl-Alt-Delete** (Ctrl + Alt + D): Enviar Ctrl+Alt+Delete para o dispositivo alvo.
- **Bloqueia o teclado e o mouse remotos** (Ctrl + Alt + K): Ativar/desativar o mouse e o teclado local do dispositivo alvo.
- **Alterna a tela inteira** (Ctrl + Alt + M): Alternar a tela do controle remoto entre o modo de janela e a modo de tela inteira.
- **Envia Ctrl+Esc** (CTRL + Alt +E): Enviar a seqüência CTRL+ESC para o dispositivo alvo.
- **Alternar mouse e modo desenhado:** Alternar entre modo desenho e modo normal do ponteiro do mouse.
- Ajustar à tela Define uma sequência de teclas de atalho para alternar entre ativar e desativar a opção Ajustar à tela.
- **Atualizar tela:** Retransmite os dados da tela do computador remoto.
- **Atualizar dados:** Envia um comando de atualização (F5) ao computador remoto.
- **Desconectar sessão:** Encerra a sessão de controle remoto atual. A janela da tela permanece aberta.

Para mudar uma tecla de atalho, clique no quadro junto à mesma e pressione a nova combinação de teclas. As teclas "Print Screen" ou "Pause/Break" não podem ser partes de uma combinação de teclas.

Enviar CTRL+ALT+DEL para dispositivos Vista e Windows 7

A política de segurança local padrão do Windows Vista e Windows 7 não permitirá a sequência Ctrl+Alt+Del vinda de uma tela de controle remoto. Para alterar isso, faça o seguinte.

Para permitir Ctrl+Alt+Del em dispositivos Vista e Windows 7

1. Na caixa de pesquisa do menu **Iniciar** digite **gpedit.msc** e pressione **Enter**.
2. Navegue para **Diretiva do computador local > Modelos administrativos > Componentes do Windows > Opções de Logon do Windows > Sequência segura de software**.
3. Clique duas vezes em **Desabilitar ou habilitar Seqüência Segura de software**.
4. Clique em **Habilitar** e na lista suspensa clique em **Serviços** ou **Serviços e aplicativos de Fácil Acesso**.
5. Clique em **OK**.

Otimização do desempenho do controle remoto

Use o diálogo **Opções** na guia **Otimizar o desempenho(Ferramentas > Opções)** para otimizar o desempenho do controle remoto nos seguintes tipos de conexão:

- Conexão lenta (modem)
- Conexão média (banda larga)
- Otimizar para conexão rápida (LAN)
- Conexão personalizada

A mudança da configuração de otimização ajusta dinamicamente a redução de cor, a visibilidade do papel de parede e os efeitos de aparência das janelas remotas (aquelas que você pode ajustar em **Propriedades de tela > Aparência > Efeitos**) como efeitos de transição para menus e dicas de ferramentas.

O controle remoto sempre usa um algoritmo de compressão altamente eficiente para dados de controle remoto. Entretanto, mesmo com compressão ele requer muitos dados para enviar informações de profundidade de cor forte. Você pode reduzir substancialmente a quantidade de dados de controle remoto necessária reduzindo a profundidade de cor mostrada na tela do controle remoto. Quando a tela reduz a profundidade de cor, a tela tem que mapear a paleta completa de cor da desktop remota para um paleta de cor reduzida na tela. Como resultado, você pode notar as cores na janela remota que não refletem de forma precisa a desktop romota. Se isso for um problema, selecione uma configuração de compressão de qualidade mais alta.

Outra forma pela qual você pode otimizar o desempenho é suprimir o papel de parede remoto. Quando você faz isso, o controle remoto não tem que enviar atualizações de papel de parede, pois partes da desktop remota estão descobertas. O papel de parede com freqüência inclui imagens de largura de banda intensiva, como fotos. Essas imagens não são compactadas muito bem e levam tempo para ser transferidas em conexões lentas.

A última maneira pela qual você pode otimizar o desempenho é utilizar o driver de espelho no dispositivo remoto. Para obter mais informações, consulte "Uso do driver de espelho" na página 250.

Interagir com usuários de dispositivos de controle remoto.

Durante uma sessão remota, você estará interagindo diretamente com o usuário final controlado remotamente ou com o dispositivo propriamente dito, ou ambos. A ferramenta de controle remoto permite que você abra uma janela de bate-papo, transfira arquivos, execute programas e reinicie o dispositivo. Você também pode salvar uma transcrição de uma sessão de bate-papo para sua referência ou como uma cópia para o usuário.

Bate-papo com dispositivos remotos

Você pode usar a tela do controle remoto para bater papo remotamente com um usuário em um dispositivo remoto. Esse recurso é útil quando você precisa dar instruções a um usuário remoto cuja conexão dial-up está usando a única linha telefônica disponível. Os usuários podem responder usando a janela de bate-papo que aparece na tela deles. Você só pode usar o bate-papo em dispositivos com o agente de controle remoto instalado. Esse recurso funciona mesmo se você não estiver vendo a tela remota do dispositivo.

É possível salvar as mensagens a partir de uma sessão de bate-papo. O texto que aparece na área cinza da sessão de bate-papo será salva em um arquivo de texto.

Para bater papo com um usuário em um dispositivo remoto

1. Clique em **Ferramentas > Bate-papo**. Uma seção da janela do visualizador torna-se uma área de bate-papo.
2. Na seção inferior esquerda da área de bate-papo, digite uma pequena mensagem. Clique em **Enviar**.

Sua mensagem será exibida em uma janela de bate-papo sdfson na tela do dispositivo remoto. Um usuário pode responder digitando uma mensagem e clicando em **Enviar**. O usuário também pode clicar em **Fechar** para sair de uma sessão de bate-papo.

Para salvar mensagens de uma sessão de bate-papo

1. Na área de bate-papo da janela do visualizador, clique em **Salvar**.
2. Na caixa de diálogo **Salvar como**, digite um nome de arquivo e clique em **Salvar**.

Transferência de arquivos para dispositivos remotos

Você pode usar a tela do controle remoto para transferir arquivos do seu computador para o dispositivo remoto. Basicamente, é como se tivesse mapeado uma unidade de um dispositivo remoto. No entanto, só é possível transferir arquivos para ou a partir dos dispositivos tendo o agente de controle remoto instalado. Esse recurso funciona mesmo se você não estiver vendo a tela remota do dispositivo.

Para transferir arquivos para um dispositivo

1. Clique em **Ferramentas > Transferência de arquivos**. Aparece o Windows Explorer.
2. Selecione um arquivo a ser transferido clicando no nome do arquivo. No menu de atalho do arquivo, clique em **Copiar**.
3. Use a barra de rolagem da árvore do Windows Explorer para ir até **Controle remoto LANDesk.** Deve aparecer o nome do dispositivo remoto que está controlando no momento.
4. No dispositivo remoto, selecione uma pasta na qual o arquivo deve ser colado e, em seguida, clique com o botão direito do mouse e selecione **Colar**.

Da mesma forma, também é possível transferir arquivos de um dispositivo remoto para o seu computador.

Execução de programas em dispositivos remotos

Você pode iniciar programas nos dispositivos remotos. Use a caixa Executar na barra de ferramentas do visualizador para inserir o caminho e nome de arquivo do programa remoto. Como o programa será iniciado no dispositivo remoto, o caminho e o nome de arquivo inseridos devem estar presentes no dispositivo remoto.

Para executar um programa em um dispositivo remoto

1. Na caixa **Executar** do visualizador, insira o caminho do programa e nome do arquivo. Se não souber, verifique a lista suspensa e clique em **Procurar**. Isso abre um diálogo que permite a busca nas pastas do dispositivo remoto.
2. Clique no botão **Executar remoto** à direita da caixa **Executar**.

Reinicialização de dispositivos remotos

Você pode usar a tela do controle remoto para reinicializar um dispositivo remotamente. No entanto, só é possível reinicializar remotamente os dispositivos que têm o agente de controle remoto instalado. Esse recurso funciona mesmo se você não estiver vendo a tela remota do dispositivo.

Para reinicializar um dispositivo remotamente

1. Clique em **Ferramentas > Reinicialização**.
2. Na caixa de edição **Tempo limite (em segundos)**, digite o tempo que um usuário terá antes que o dispositivo seja reinicializado. A demora máxima é de 300 segundos.
3. Na caixa **Aviso ao usuário remoto**, digite uma breve mensagem de aviso, que o usuário verá antes de o dispositivo ser reinicializado remotamente.
4. Você pode salvar suas configurações clicando em **Salvar configurações**.
5. Clique em **OK**.

A mensagem de aviso aparecerá no dispositivo com contagem regressiva, mostrando quanto tempo ainda falta para a reinicialização. O usuário pode clicar em **OK** para reinicializar imediatamente ou em **Cancelar** para não aceitar a solicitação. Se o usuário rejeitar a solicitação, uma caixa de diálogo aparecerá no seu computador para avisá-lo. Se a inicialização ocorrer, você verá uma mensagem na área de mensagens de sessão da janela do visualizador.

Alteração da segurança do controle remoto do dispositivo

O Management Suite possui um alto nível de controle sobre os dispositivos quando são concedidos direitos de acesso. O dispositivo controla a segurança do acesso remoto. Ele armazena as configurações de segurança de acesso remoto no registro.

Você pode mudar as configurações do controle remoto e o modelo de segurança nos clientes ao atualizar as definições de configuração do agente (**Ferramentas > Configuração do agente**) e do menu de atalho da configuração atualizada, clicando em **Agendar atualização**. Quando distribuir a atualização aos dispositivos, o seus agentes usarão as configurações que você especificou.

Para obter mais informações, consulte "Distribuição do controle remoto" na página 122.

Uso do log de controle remoto

Por padrão, o Management Suite registra as ações de controle remoto, incluindo o dispositivo controlado remotamente e o console que faz o controle remoto. Você pode desativar o log do controle remoto se quiser ou pode purgar as entradas de log do controle remoto mais antigas que a data que especificar.

Se o login estiver habilitado, você pode ver os seguintes relatórios de controle remoto (**Ferramentas > Relatórios/Monitoramento > Relatórios** e na ferramenta **Relatórios**, clique em **Relatórios > Relatórios padrão > Controle remoto**):

- Histórico do controle remoto por usuário
- Resumo do controle remoto
- (A lista de relatórios padrão pode variar de um lançamento para outro)

Para habilitar ou desabilitar o log do controle remoto

1. No console do Management Suite, clique em **Configurar > Log do controle remoto**.
2. Selecione ou limpe a opção **Habilitar histórico do controle remoto**, conforme sua preferência.

Para purgar o log do controle remoto

1. Clique em **Configurar > Login do controle remoto**.
2. Digite a data que quer purgar. Todas as entradas mais antigas que esta data serão excluídas.
3. Clique em **Excluir histórico** para executar a tarefa de exclusão.

Se os dispositivos gerenciados estiverem usando o modelo de controle remoto "Windows NT security", há algumas etapas adicionais necessárias para assegurar que os relatórios de controle remoto mostrem as informações corretas. No modelo "Windows NT security", tanto o operador do controle remoto como os dispositivos precisam ser membros do mesmo domínio do Windows. Pode ser necessário também verificar se as contas de domínio dos operadores de controle remoto estão no grupo **Operadores de controle remoto** na página de configuração do agente de **Controle remoto**. Se isso não for feito, o relatório de controle remoto mostrará o usuário local como operador do controle remoto em vez do verdadeiro operador.

Habilitação do login de controle remoto em um arquivo de texto.

A habilitação do login de controle remoto em um arquivo de texto pode ser feita pela criação das seguintes chave de registro nos dispositivos gerenciados:

- Crie o seguinte valor DWORD e defina-o como 1: HKLM\SOFTWARE\LANDesk\Instant Support Suite Console\Container\LogSessionMessages.
- Crie o valor de string a seguir em um caminho UNC acessível (incluindo uma contrabarra) a partir de um dispositivo gerenciado: HKLM\SOFTWARE\LANDesk\Instant Support Suite Console\LogPath.

O nome do arquivo de log é issuser.log.

Mudança do modo de controle remoto nos dispositivos alvo

Os agentes de controle remoto LANDesk nos dispositivos aceitam dois tipos de conexão:

- Conexões diretas da janela da tela do controle remoto LANDesk.
- Conexões Management Gateway através de um gateway de gerenciamento.

O agente de controle remoto só detecta um tipo de conexão. Se quiser mudar o tipo de conexão que o agente detecta, clique duas vezes no status do ícone do controle remoto na bandeja de sistema do dispositivo alvo e clique em **Mudar o modo**. Isso alterna o agente entre o modo direto e o modo gateway. O texto no diálogo de status do controle remoto mostra o modo atual do agente de controle remoto. Você pode deixar seus usuários alternar entre os modos ou pode fazer isso através da sessão de controle remoto. Se você fizer isso através da sessão de controle remoto, a sessão desconectará assim que você clicar no botão **Mudar o modo**.

O LANDesk System Manager não suporta o Management Gateway, por isso esse botão aparecerá esmaecido nos dispositivos gerenciados pelo System Manager.

Personalização dos agentes de controle remoto e da tela

A tela do controle remoto tem opções de linha de comando que você pode usar para personalizar a maneira como ela funciona. Se necessário, é possível também ajustar as chaves de registro do agente de controle remoto nos dispositivos. Normalmente essas chaves de registro são definidas pela configuração do agente do controle remoto que você distribuir para o dispositivos.

Opções da linha de comandos da tela

Você pode iniciar a tela do controle remoto usando uma opção de linha de comando que abre imediatamente a janela, conecta-o com um dispositivo específico e ativa os recursos desejados da tela como, por exemplo, controle remoto, bate-papo, transferência de arquivo ou reinicialização do dispositivo. O programa do controle remoto, isscntr.exe, está na pasta principal de programa do ManagementSuite.

As opções de linha de comando de controle remoto usam a seguinte sintaxe:

```
isscntr /a<endereço> /c<comando> /l /s<servidor núcleo>
```

Se o servidor núcleo usa segurança baseada em certificados ou segurança integrada para o controle remoto, deve usar o parâmetro /s para especificar o o servidor núcleo.

Opção	Descrição
/a<endereço>	Contata um dispositivo em um endereço TCP/IP em particular. O endereço TCP/IP pode incluir endereços de estilo numérico e de nome, separados por ponto e vírgula. Você também pode especificar o nome de host.
/c<comando>	Inicia a tela do comando remoto e executa um recurso específico. (Consulte os nomes de comando abaixo.) Você pode especificar múltiplos argumentos /c em uma linha de comando. Por exemplo: isscntr /agamma /c"remote control" /c"file transfer" Os seguintes recursos estão disponíveis: **Controle remoto**: abre a janela do controle remoto **Reinicialização:** reinicializa o dispositivo específico **Bate-papo:** abre uma janela de bate-papo **Transferência de arquivo:** abre uma sessão de transferência de arquivo **Informações do sistema**: Abre uma janela com informações sobre o dispositivo, inclusive SO, memória e espaço no disco rígido
/l	Limita a interface da tela de modo a mostrar apenas os recursos que você especificar com /c.
/s<servidor núcleo>	Se estiver usando uma segurança baseada em certificado, use esta opção para especificar o servidor núcleo com o qual autenticar. Esta opção é útil se estiver controlando remotamente clientes em um ambiente núcleo variado. Se o servidor núcleo usa segurança baseada em certificados ou segurança integrada para o controle remoto, deve usar o parâmetro /s para especificar o o servidor núcleo.

Exemplo 1

Abre a janela do visualizador. As mudanças feitas, por exemplo, o redimensionamento da janela de mensagens da conexão ou a configuração de opções de desempenho da última vez que a janela foi usada são retidas.

```
isscntr
```

Exemplo 2

Inicia uma sessão de controle remoto conectando ao dispositivo denominado “gamma". (Observe que não há espaço e nem pontuação entre "/a" e "gamma".)

```
isscntr /agamma /c"controle remoto"
```

Exemplo 3

Inicia uma sessão de controle remoto e bate-papo conectando-se ao dispositivo denominado “gamma". O controle remoto tenta primeiro resolver o nome "gamma". Se isso falhar, ele tenta conectar ao endereço numérico 10.10.10.10:

```
isscntr /agamma;10.10.10.10 /c"controle remoto" /c"bate papo"
```

Exemplo 4

A porta 9535 é usada para comunicação entre a tela e os computadores agentes. Se os dispositivos executando o issuser.exe são configurados para usar uma porta diferente da porta 9535, a porta deve ser passada como parte do endereço dado ao isscntr.exe. Por exemplo, para controlar remotamente um dispositivo com o endereço 10.4.11.44, onde o issuser.exe está configurado para usar a porta 1792 como porta de verificação, a linha de comando deveria ser:

```
isscntr /a10.4.11.44:1792 /c"controle remoto"
```

Solução de problemas nas sessões de controle remoto

Essa seção descreve problemas que podem aparecer ao controlar remotamente um dispositivo e suas possíveis soluções.

Não consigo controlar remotamente um dispositivo

Verifique se o dispositivo tem os agentes LANDesk carregados.

Para verificar se os agentes LANDesk estão carregados:

- Na tela de rede do console, clique em **Propriedades** no menu de atalhos do dispositivo. Clique na guia **Agentes** para ver os agentes carregados.

Para carregar o agente Controle remoto

- Crie uma tarefa de configuração do agente no console e envie-a ao dispositivo ou mapeie uma unidade a partir do dispositivo ao servidor núcleo e execute a tarefa de configuração do dispositivo apropriada.

Não é possível transferir arquivos entre o console e o dispositivo alvo

Verifique se você está executando o Norton AntiVirus e se o Integrity Shield está ativado. Se o Integrity Shield estiver ativado, você precisará ter privilégios temporários que permitam copiar para o diretório que o Integrity Shield está protegendo.

Distribuição de softwares/Distribuição de pacotes/Métodos de entrega

Sobre a distribuição de softwares

A tecnologia de distribuição de software do LANDesk Management Suite ajuda o pessoal de TI a implementar a automação controlada para a distribuição e instalação rápida e eficiente de softwares, atualização de vírus e segurança e gerenciamento de patch de aplicativos em ambientes mistos de rede. A tecnologia é baseada em um modelo modular, baseado em tarefa, que pode melhorar consideravelmente a eficiência no planejamento, programação e gerenciamento das distribuições de softwares. Pacotes, métodos de distribuição, scripts de distribuição e seleção de alvos são gerenciados separadamente para aumentar a flexibilidade .

Principais recursos e benefícios

- **Mapeamento de código de retorno:** Define códigos de retorno para melhorar a exatidão da instalação do aplicativo.
- **Suporte MSI nativo:** Copiar e colar as chamadas das linhas de comando do MSI.
- **Fluxo de trabalho simplificado:** Torna os pacotes de instalação mais fáceis e rápidos de instalar.
- **Controle de largura de banda simplificados:** Personalizar configurações adequadamente.
- **Modelagem baseada em tarefas:** Separa a construção de pacotes e os métodos de distribuição para melhorar a eficiência.
- **LANDesk® Targeted Multicast™: Distribua** grandes pacotes para vários usuários com largura de banda mínima e sem a necessidade de hardware dedicado ou reconfiguração de roteadores.
- **LANDesk® Peer Download™:** Permite que você acesse pacotes que já foram distribuídos a uma subrede.
- **Verificação de pré-requisitos e cadeia de pacotes:** Instala os pacotes de pré-requisitos e permite que você instale automaticamente pacotes múltiplos em uma única operação.
- **Agendador de tarefas:** Integrado com os bancos de dados de serviço de diretórios e inventários de recursos para ajudá-lo na seleção de alvos.
- **Distribuição agnóstica de pacotes:** Distribui todo tipo de pacote e permite o acesso ao suporte MSI a arquivos múltiplos.
- **Portal de auto-serviço:** Reduz incidentes de help-desk, autoriza usuários a iniciar instalações aprovadas e permite a rápida solução de problemas através de histórias detalhadas.
- **Distribuição baseada em diretiva:** Dispõe múltiplos pacotes de software em uma única diretriz e garante que os pacotes estão disponíveis para atualizações futuras e reaplicação, se necessário.

Em Management Suite, distribuição de software consiste em três etapas principais:

1. **Criação ou obtenção de um pacote de software** O pacote de software pode ser um ou mais arquivos MSI, um executável, um arquivo de lote, um pacote Macintosh, um pacote de RPM Linux, um pacote de host de script Windows, um pacote de virtualização de aplicativos ou um pacote criado com o criador de pacotes do Management Suite. Coloque o pacote no seu servidor de distribuição.

2. **Crie um pacote de distribuição (Ferramentas > Distribuição > Pacotes de distribuição)**. O pacote de distribuição contém os arquivos e as configurações necessárias para se instalar um pacote de software específico, por exemplo, o nome do pacote, quaisquer dependências ou pré-requisitos, parâmetros de linha de comando, arquivos adicionais necessários para a instalação do pacote, etc. Essas configurações são armazenadas no banco de dados e criam um pacote de distribuição. Uma vez criado um pacote de distribuição, as informações são armazenadas no banco de dados e podem ser facilmente utilizadas em múltiplas tarefas.
3. **Crie um método de distribuição (Ferramentas > Distribuição > Métodos de distribuição)**. O método de distribuição define a forma como um pacote será enviado aos dispositivos. Estas opções não estão associadas a nenhum pacote de distribuição específico. As opções contêm Multidifusão dirigida e distribuições por envio e/ou por diretiva. Não crie um método de entrega todas as vezes que desejar distribuir um pacote. Métodos de entrega permitem que você defina as melhores práticas para a distribuição de software. O ideal é criar um gabarito (ou modelo) de método de entrega para ser reusado para distribuições que utilizam o mesmo método de entrega.
4. **Agende o trabalho de distribuição na janela de Tarefas agendadas (Ferramentas > Distribuição > Tarefas agendadas)**. Especifique o pacote de distribuição, o método de entrega, os dispositivos que precisam receber o pacote de distribuição e quando a tarefa deverá ser executada.
5. Quando ocorre o horário agendado, o serviço agendador inicia o manipulador da tarefa agendada que distribui o pacote usando as opções selecionadas no método de entrega. Essas ações remotas incluem o seguinte:

    - Se um método de entrega que usa multidifusão é selecionado, é usada a multidifusão.
    - Se for selecionado um método de distribuição por envio, o serviço do agendador contata o agente de distribuição de software em cada dispositivo e o informa que o pacote está pronto para instalação.
    - Se for selecionado um método de entrega com base em diretiva, o pacote torna-se disponível para download .

6. O agente da Distribuição de software obtém o pacote de seu cache local, de um parceiro na rede, ou do servidor de distribuição e o processa no dispositivo, instalando ou removendo arquivos de pacote.
7. Depois que o pacote é processado, o agente de distribuição de software envia o resultado ao servidor núcleo, onde ele é registrado no banco de dados núcleo.

A separação das tarefas de distribuição em duas partes, distribuição de pacotes e métodos de entrega, simplifica o processo de distribuição. Agora você pode criar gabaritos de métodos de distribuição que são independentes de um pacote específico. Por exemplo, você pode criar um modelo de método de distribuição de Multidifusão dirigida padrão e sempre que tiver um pacote que desejar distribuir, ele pode ser distribuído com o uso desse gabarito sem que você tenha de reconfigurar o pacote ou o método de distribuição.

Se você tiver pessoas diferentes para criar e distribuir pacotes na sua organização, essas mudanças ajudam a simplificar a divisão de funções e tarefas. Os criadores de pacotes podem agora trabalhar independentes dos distribuidores de pacotes.

Entendendo os tipos de pacotes de distribuição

A distribuição de software suporta os seguintes tipos de pacotes:

MSI

Esses são pacotes no formato do Windows Installer. Você precisa usar uma ferramenta de terceiros para criar os pacotes MSI. Esses pacotes consistem em um arquivo primário .msi e podem conter arquivos de suporte e transformações. As transformações personalizam a maneira como os pacotes MSI são instalados. Se o seu pacote MSI consiste em múltiplos arquivos, adicione todos eles no diálogo **Pacote de distribuição**.

Executável

Para um pacote executável ser usado pela distribuição de software, é necessário satisfazer os seguintes critérios:

- O executável não pode sair antes da instalação estar completa.
- O executável deve retornar zero (0) para uma instalação bem sucedida.

Desde que o executável satisfaça esses dois critérios, qualquer executável pode ser usado para a instalação do pacote. Você pode incluir arquivos adicionais para os pacotes executáveis.

Arquivo em lote

Os pacotes de arquivo em lote são baseados em um arquivo em lote do Windows/DOS. Você pode incluir arquivos adicionais para esses pacotes de distribuição. O status de conclusão bem sucedida do pacote de arquivo em lote é baseado no valor da variável do ambiente de sistema de errorlevel quando o arquivo em lote tiver terminado a execução.

Macintosh

Qualquer Macintosh arquivo pode ser baixado, embora o Management Suite não baixe diretórios. Os pacotes de instalação (.pkg) podem conter diretórios. Eles devem ser compactados. Se o arquivo baixado tiver a extensão .sit, .zip, .tar, .gz, .sea, ou .hqx, o Management Suite descompactará o arquivo antes de retornar. (Os usuários devem confirmar se a opção "verificação de novas versões" do Stuffit Expander está desativada; caso contrário, uma caixa de diálogo provavelmente interromperá a execução do script.)

RPM Linux

Esses são pacotes no formato RPM Linux. Esses pacotes devem ser armazenados em um compartilhamento de web para a distribuição RPM Linux funcionar.

LANDesk Application Virtualization

O LANDesk Application Virtualization usa a tecnologia Thinstall para virtualizar um aplicativo, armazenando-o em único arquivo executável independente que contém o aplicativo e as dependências de DLL/driver de dispositivos. Os aplicativos virtualizados são executados em um ambiente isolado sem mudar a instalação do Windows.

Os aplicativos virtualizados podem ser executados em dispositivos bloqueados sem a necessidade de privilégios adicionais.

Geralmente, os aplicativos virtualizados consistem em um ou mais arquivos executáveis. A distribuição de software pode ser usada para implantar os arquivos executáveis de aplicativos virtualizados em dispositivos gerenciados. Qualquer um dos método de entrega de distribuição de software pode ser usado com os pacotes de aplictivos virtualizados, inclusive o comando Run (Executar) da origem. Ao distribuir um pacote de aplicativo virtualizado para execução da origem, os dispositivos gerenciados usam um ícone de atalho para executar o aplicativo virtualizado pela rede.

Pacote do Windows Script Host (.wsf)

Os Pacotes de Windows Script Host (WSH) são a nova alternativa de software da Microsoft aos arquivos de lote que com frequência são usados para automatizar tarefas semelhantes como mapear unidades, copiar arquivos ou modificar chaves do registro. Os arquivos WSH são mais comumente usados com o Jscript (.JS) e o VBScript (.VBS). Uma vantagem importante do pacote de Host de script Windows em relação ao pacote .bat é que ele permite ao usuário combinar múltiplos idiomas em um único arquivo usando a extensão de arquivo independente de idioma (wsf). Esses pacotes podem, com frequência, ser criados em Notepad, um editor HTML, Microsoft Visual C++ ou Visual InterDev.

Pacote SWD

Esses são pacotes compilados com o LANDesk Enhanced Package Builder antigo (instalado separadamente). Embora o Enhanced Package Builder não seja mais vendido com o Management Suite, a LANDesk Software continua a dar duporte à distribuição de arquivos criados com ele. Eles são arquivos executáveis que têm propriedades que os identificam exclusivamente como pacotes de distribuição de software (SWD).

Compreensão dos métodos de entrega disponíveis na distribuição

A distribuição de software fornece os seguintes métodos de entrega:

- **Por envio:** Os pacotes podem ser distribuídos por multidifusão para os dispositivos gerenciados. O servidor núcleo então inicia a instalação do pacote nos dispositivos gerenciados.
- **Diretiva:** O servidor núcleo torna os pacotes disponíveis para download. Quando um dispositivo gerenciado verifica as diretivas disponíveis, o pacote é retornado. Dependendo do tipo de diretiva, os dispositivos podem instalar o pacote automaticamente ou disponibilizar o pacote aos usuários para ele instalarem quando quiserem.
- **Envio suportado por diretiva:** Modelo combinado de distribuição por envio e diretiva. Primeiro, a distribuição de software tenta instalar o pacote em todos os dispositivos na lista de alvos. Deste modo, você pode fazer uma distribuição inicial usando a Multidifusão dirigida. Em segundo lugar, quaisquer dispositivos que não tiverem recebido o pacote, ou que tiverem sido incluídos na lista de alvos posteriormente (no caso de uma lista de alvos dinâmica), recebem o pacote quando o agente do gerenciamento baseado em diretivas no dispositivo o solicitar. Em geral, este é o método recomendado de entrega.
- **Multidifusão (somente cache):** Os pacotes são enviados para dispositivos alvo e nenhuma outra ação é executada no dispositivo gerenciado. Como resultado, o pacote é colocado em cache local nos dispositivos gerenciados. Use essa opção para fazer multidifusão do pacote para alguns dispositivos em cada domínio de multidifusão. Você pode, assim, criar uma tarefa que utiliza a opção **Download de parceiro (só instala de um cache ou de um parceiro)**. Isso permite regular a largura de banda de rede usada para a distribuição de forma a não permitir a extensão pelos domínios de multidifusão.

NOTA: A LANDesk incluíu configurções de método de entrega padrão para cada um desses tipos de métodos. Esse métodos padrão têm configurações padrão que devem funcionar na maioria dos ambientes. Se você quiser modificar um desses padrões, você pode precisar usar os recursos copiar e colar para criar um método de entrega duplicado que você pode renomear, preservando os padrões para referência futura.

Definir um servidor de entrega para a distribuição de softwares baseado em URL

O servidor de entrega é o servidor que armazena os pacotes de distribuição de software. Pode ser um servidor de Web ou um servidor de arquivos Windows. Para melhores resultados, recomendamos que os pacotes sejam baseados em URL. Em geral, a configuração correta de um URL dá menos trabalho do que a configuração de um caminho UNC.

Os compartilhamentos de pacote HTTP precisam ter uma Conta de Convidado à Internet adicionada com pelo menos, privilégios de leitura, já que os pacotes serão acessados através de HTTP anônimo.

Para configurar um Servidor da Web para distribuição de software

Estas etapas ensinam a criar um diretório virtual em um Servidor da web e a ativá-lo para navegação. Em geral, diretórios virtuais precisam permitir leitura e pesquisa no diretório, e o acesso anônimo ao diretório virtual deve estar ativado. A permissão de execução não deve ser ativada. Caso contrário, o compartilhamento não funcionará corretamente. Você também pode decidir desativar as permissões de gravação para que os dispositivos não mudem o conteúdo do diretório.

1. Crie um diretório no Servidor da web no qual deseja armazenar os pacotes de distribuição de software. O local usual para esse diretório em um Servidor da web IIS é um subdiretório no diretório c:\inetpub\wwwroot.
2. Copie os pacotes para esse diretório.
3. No Painel de controle, clique duas vezes em **Ferramentas administrativas** e, em seguida, em **Gerenciador de serviços de Internet**.
4. No painel da direita, clique duas vezes no ícone com o nome do dispositivo e clique em **Site da web padrão**.
5. Em uma área vazia do painel da direita, clique com o botão direito do mouse e selecione **Novo**, em seguida clique em **Diretório virtual**.
6. No assistente, clique em **Avançar** e digite um alias para o diretório. Clique em **Avançar**.
7. Digite o caminho ou navegue até um caminho e clique em **Avançar**.
8. Na caixa de diálogo Permissões de acesso, ative **Executar script** e **Procurar**. Isso permite que você procure pacotes ao criar script de pacote de distribuição. Clique em **Avançar** e em **Concluir**.
9. No menu de atalho do diretório virtual criado, clique em **Propriedades**.
10. Na guia **Documentos**, desmarque a opção **Ativar página de conteúdo padrão** e clique em **OK**. As páginas padrão podem interferir com a mesma habilidade do compartilhamento para fornecer um diretório que pode ser navegado.
11. Na guia **Segurança de diretório**, clique em **Editar** na caixa **Acesso anônimo e controle de autenticação**. Certifique-se que **Autenticação Integrada do Windows** esteja marcada. Certifique-se também de que **Autenticação Digest para servidores de domínio do Windows** esteja desmarcada.
12. Para ativar **Porta 80** no servidor da Web, no painel da esquerda, clique com o botão direito do mouse em **Site padrão**.
13. Clique em **Propriedades**. Na caixa de diálogo **Identificação do site**, a caixa de diálogo **Porta TCP** deve exibir 80, caso contrário, clique em Avançado para adicionar a porta.

14. Verifique se o site está disponível abrindo um browser e digitando o URL do seu servidor da Web e do diretório virtual. Por exemplo, se o nome do seu servidor da Web for Teste e o nome do diretório virtual for Pacotes, digite o seguinte URL:

    http://Test/Packages

    Uma lista dos pacotes que você copiou nesse diretório deve ser exibida.

O tamanho e o número de pacotes que podem ser colocados nesse diretório dependem apenas do espaço em disco disponível. Podem ser criados subdiretórios para agrupar pacotes logicamente. Cada subdiretório que é criado deve ter o conjunto de permissões de acesso, conforme descrito na tarefa "Para configurar um servidor de web para distribuição de software" acima.

Assim que você copiar os pacotes em um compartilhamento de pacotes de um Servidor de web, eles estarão prontos para serem copiados para os dispositivos alvo. Quando agendado, o caminho URL ou UNC do pacote é transmitido ao SDClient.exe (o agente do dispositivo) como um parâmetro de linha de comandos. O SDClient.exe gerencia a transferência de arquivos, inicia a instalação e informa o status. Embora o protocolo HTTP seja usado para a transferência de arquivos, o relatório de status é retornado através do agente padrão.

O Servidor de web comunica-se com o dispositivo para garantir que o pacote seja copiado corretamente. Se a transmissão do pacote for interrompida durante o download, o servidor da Web poderá usar o protocolo HTTP para reiniciar o download no ponto em que foi interrompido. Entretanto, o servidor Web não verifica se o pacote foi instalado corretamente. Esse tráfego é baseado em TCP e retorna o status ao servidor núcleo usando o agente LANDesk padrão.

Configuração de servidores Web do IIS para a distribuição de software

Quando hospedar pacotes em um servidor web Microsoft IIS, há algumas configurações adicionais necessárias:

- Configure o diretório virtual que hospeda seus pacotes.
- Registre um tipo de MIME com o IIS.

O IIS 6 trabalha com diretórios virtuais de forma diferente do IIS 5 (o IIS 5 era o servidor de web do Windows 2000). Em um servidor IIS 6, se você selecionar um diretório e do seu menu de atalho, torná-lo um compartilhamento de web, o diretório registrar-se-á no IIS 6 como um aplicativo de web, e não como um diretório virtual. O problema é que, como um aplicativo de Web, ao tentar selecionar um arquivo executável, o servidor da Web tentará executar o arquivo como um aplicativo de Web e não efetuar o download do arquivo para o usuário.

A solução é ir ao IIS, mudar o diretório compartilhado de um aplicativo da Web para um diretório virtual e desativar as permissões de execução.

Na hospedagem de arquivos em um servidor IIS 6, os arquivos que não tiverem um tipo MIME registrado acarretarão um erro 404 de HTTP, Arquivo não encontrado. Isso resultará na multidifusão e/ou na falha da instalação do arquivo a menos que registre tipos de arquivo MIME.

Para registrar tipos de arquivo MIME

1. Inicie o Gerenciador do IIS (Internet Information Services).
2. Expanda o computador local na árvore.

3. Clique em **Sites > Site da web Padrão**.
4. No menu de atalho do compartilhamento de Web, clique em **Propriedades**.
5. Clique na guia **Cabeçalhos HTTP**.
6. Clique em **Tipos MIME**.
7. Clique em **Nova**.
8. Na caixa **Extensão**, digite um asterisco (.*).
9. Na caixa **Tipo MIME**, digite **aplicativo/stream-octeto**.
10. Clique em **OK** duas vezes e aplique as alterações.

Definir um servidor de entrega para a distribuição de softwares baseado em UNC

O servidor de entrega é o servidor que armazena os pacotes de distribuição de software. Pode ser um servidor de Web ou um servidor de arquivos Windows. Para melhores resultados, recomendamos que os pacotes sejam baseados em URL. Em geral, a configuração correta de um URL dá menos trabalho do que a configuração de um caminho UNC.

Os compartilhamentos de pacotes UNC precisam ter o grupo de Computadores do Domínio adicionados com pelo menos, privilégios de leitura.

Os dispositivos que não têm um navegador devem receber pacotes de distribuição de um caminho UNC em um servidor de rede Windows. Esse diretório pode ser o mesmo que você usou para instalar o servidor Web. Se estiver usando servidores preferenciais, configure ali as credenciais de autenticação para o seu compartilhamento de pacote UNC. Você não terá que configurar um compartilhamento de sessão nula.

Se não estiver usando servidores preferenciais ou credenciais dos mesmos, terá que tornar o pacote como de compartilhamento de sessão nula, o que permite aos usuários o acesso ao compartilhamento sem ter que fornecer credenciais alternativas. Use o utilitário SysShrs.exe para criar uma pasta de compartilhamento de sessão nula.

Para configurar um servidor de rede para a distribuição de software

1. Para configurar uma pasta compartilhada no servidor de rede, clique com o botão direito do mouse na pasta a ser compartilhada e clique em **Compartilhamento**.
2. Clique em **Compartilhar esta pasta** e em **Permissões**.
3. Adicione os grupos **Todos** e **Convidado**, mas conceda a eles apenas as permissões de leitura. No ambiente de domínio, adicione também o grupo **Computadores do domínio** e conceda apenas permissões de leitura. Aplique as alterações.
4. Configure credenciais do servidor preferencial de pacotes, conforme descrito em "Configurar servidores preferenciais " na página 867.
5. Copie os pacotes de distribuição de software para esse diretório no servidor de rede.

O tamanho e o número de pacotes que podem ser armazenados no servidor de rede dependem somente do espaço em disco disponível.

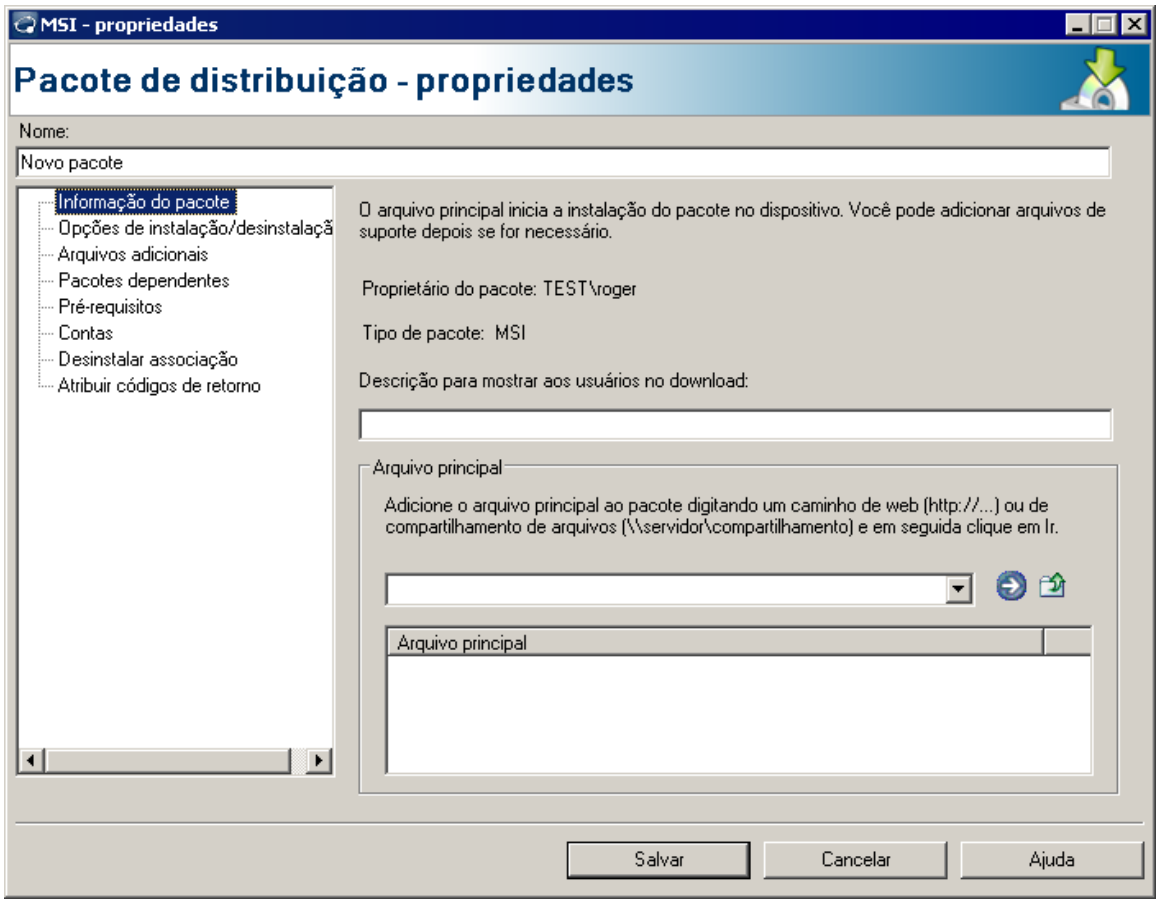
Distribuir um pacote

Um pacote de distribuição consiste em um arquivo de pacote que você deseja distribuir, arquivos adicionais necessários ao pacote e configurações que descrevem os componentes de pacote e comportamento. É necessário criar o pacote antes de poder criar a definição de pacote para ele.

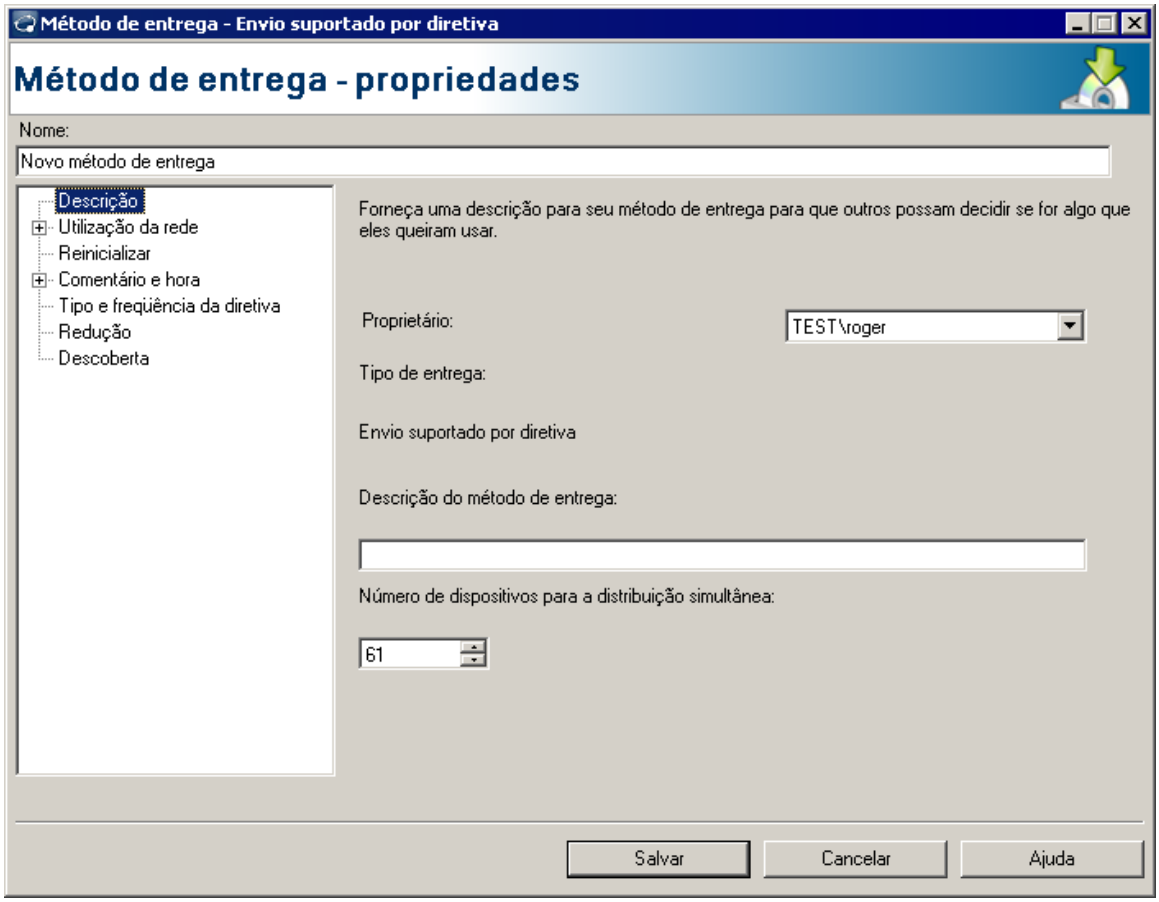
Estas instruções explicam como criar um script de distribuição do pacote. Para o script ser executado corretamente, o pacote de distribuição de software deve existir em um servidor de rede ou em um Servidor web e os dispositivos devem ter um agente de distribuição de software instalado.

Há três etapas principais necessárias para distribuir um pacote para dispositivos.

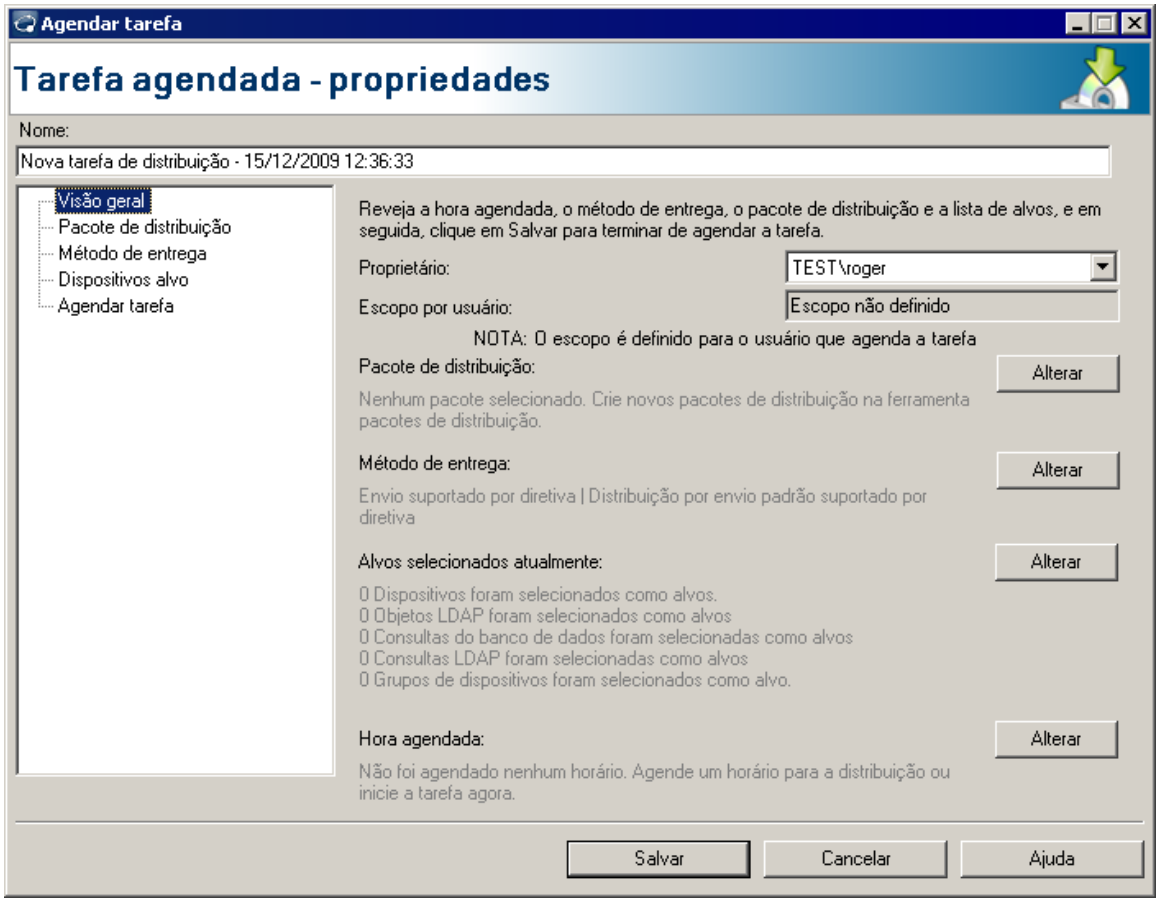
Etapa 1: Crie um script de pacote de distribuição para o pacote que desejar distribuir.


MSI - propriedades
Pacote de distribuição - propriedades
Nome:
Novo pacote
Informação do pacote
Opções de instalação/desinstalaçã
Arquivos adicionais
Pacotes dependentes
Pré-requisitos
Contas
Desinstalar associação
Atribuir códigos de retorno
O arquivo principal inicia a instalação do pacote no dispositivo. Você pode adicionar arquivos de suporte depois se for necessário.
Proprietário do pacote: TEST\roger
Tipo de pacote: MSI
Descrição para mostrar aos usuários no download:
Arquivo principal
Adicione o arquivo principal ao pacote digitando um caminho de web (http://...) ou de compartilhamento de arquivos (\\servidor\compartilhamento) e em seguida clique em Ir.
Arquivo principal
Salvar
Cancelar
Ajuda

Etapa 2: Escolha o método de entrega.



Etapa 3: Agendamento do pacote e método para a distribuição.


Agendar tarefa
Tarefa agendada - propriedades
Nome:
Nova tarefa de distribuição - 15/12/2009 12:36:33
Visão geral
Pacote de distribuição
Método de entrega
Dispositivos alvo
Agendar tarefa
Reveja a hora agendada, o método de entrega, o pacote de distribuição e a lista de alvos, e em seguida, clique em Salvar para terminar de agendar a tarefa.
Proprietário:
TEST\roger
Escopo por usuário:
Escopo não definido
NOTA: O escopo é definido para o usuário que agenda a tarefa
Pacote de distribuição:
Alterar
Nenhum pacote selecionado. Crie novos pacotes de distribuição na ferramenta pacotes de distribuição.
Método de entrega:
Alterar
Envio suportado por diretiva | Distribuição por envio padrão suportado por diretiva
Alvos selecionados atualmente:
Alterar
0 Dispositivos foram selecionados como alvos.
0 Objetos LDAP foram selecionados como alvos
0 Consultas do banco de dados foram selecionadas como alvos
0 Consultas LDAP foram selecionadas como alvos
0 Grupos de dispositivos foram selecionados como alvo.
Hora agendada:
Alterar
Não foi agendado nenhum horário. Agende um horário para a distribuição ou inicie a tarefa agora.
Salvar
Cancelar
Ajuda

Para criar um script de pacote de distribuição

1. Crie o pacote a ser distribuído.
2. Clique em **Ferramentas > Distribuição > Pacotes de distribuição**.
3. Do menu de atalho do grupo de pacote desejado, clique em **Novo pacote de distribuição** > o tipo de pacote que deseja criar.
4. Na caixa de diálogo **Pacote de distribuição**, insira as informações do pacote e altere as opções que desejar. Observe que é necessário inserir o nome do pacote, a descrição e o arquivo primário. Para obter mais informações sobre cada página, clique em **Ajuda**.
5. Clique em **OK** quando tiver concluído. O seu script será exibido sob o item da árvore para o tipo de pacote e o proprietário selecionados.

NOTA: A LANDesk incluíu configurções de método de entrega padrão para cada tipo de método. Esse métodos padrão têm configurações padrão que devem funcionar na maioria dos ambientes. Se você quiser modificar um desses padrões, você pode precisar usar os recursos copiar e colar para criar um método de entrega duplicado que você pode renomear, preservando os padrões para referência futura.

Para criar um método de entrega (só necessário se um método de entrega padrão não for ideal no seu ambiente)

1. Se você já configurou um método de distribuição que deseja usar ou está usando um dos métodos de entrega padrão, avance para o procedimento seguinte, "Para agendar uma tarefa de distribuição".
2. Clique em **Ferramentas > Distribuição > Métodos de entrega**.
3. Clique com o botão direito do mouse no método de entrega que desejar usar e clique em **Novo método de entrega**.
4. Na caixa de diálogo **Método de entrega**, insira as informações de distribuição e altere as opções que desejar. Para obter mais informações sobre cada página, clique em **Ajuda**.
5. Clique em **OK** quando tiver concluído. O seu script aparece sob o item da árvore do método de distribuição e proprietário selecionado.

Para agendar uma tarefa de distribuição

1. Clique em **Ferramentas > Distribuição > Tarefas agendadas**.
2. Clique no botão **Criar tarefa de distribuição de software** na barra de ferramentas.
3. Na página **Pacote de distribuição**, selecione o pacote de distribuição que criou.
4. Na página **Método de entrega**, selecione o método de entrega que desejar usar.
5. Clique em **Salvar** para salvar suas mudanças.
6. Na tela de rede, arraste alvos na tarefa e na janela **Tarefas agendadas**. Os alvos podem incluir dispositivos individuais, grupos de computadores, objetos LDAP (usuário, máquina e grupo), consultas LDAP e consultas de inventário.
7. No menu de atalho dessa pasta, clique em **Propriedades**.
8. A página **Dispositivos alvo** mostra os dispositivos que receberão nesta tarefa.
9. Na página **Agendar tarefa**, insira o nome e o agendamento da tarefa.
10. Volte para a página **Visão geral** e confirme que a tarefa foi configurada da forma que você quer.
11. Clique em **Salvar** quando terminar.

Veja o andamento da tarefa na janela **Tarefas agendadas**.

Trabalhando com proprietários de distribuição e direitos

Nos ambientes onde há muitos usuários do Management Suite, pode ficar confuso saber por que pacotes de distribuição, métodos de entrega e tarefas agendadas cada usuário é responsável. Para ajudar a resolver esse problema, o Management Suite torna o usuário que criou o pacote de distribuição, o método de entrega ou a tarefa agendada o proprietário padrão do item. Somente o proprietário e os usuários da configuração RBA Administradores/Distribuição de software podem ver esses itens privados.

Os itens privados aparecem nas árvores **Meus métodos de distribuição**, **Meus pacotes** ou **Minhas tarefas**. Os usuários administrativos podem ver itens de todos os usuários nas árvores **Todos os pacotes de distribuição**, **Todos os métodos de distribuição** e **Todas as tarefas**.

Quando os usuários criam um item de distribuição, a página **Descrição** tem uma opção **Proprietário**. Os usuários podem selecionar **Público** se quiserem que todos os usuários do console vejam aquele item. Os administradores podem selecionar um usuário específico, além do **Público**.

Para encontrar mais informações sobre a administração de baseada em função com distribuição de software, consulte "Distribuição de software" na página 52.

Uso de vários pacotes de distribuição em uma tarefa

As tarefas de distribuição de software baseadas em envio, diretiva e envio suportado por diretiva podem conter um pacote preliminar e um pacote final. Ao usar pacotes múltiplos, os pacotes são instalados em ordem, um por vez. O pacote anterior deve retornar um status bem sucedido de tarefa em todos os dispositivos alvo antes do próximo pacote começar a instalar.

Pacotes preliminares e finais são úteis nos casos onde você desejar executar comandos antes e/ou depois do pacote principal. Por exemplo, você poderia criar um pacote de arquivo em lote que executa comandos para configurar o dispositivo alvo para o pacote principal. Após o pacote principal terminar a instalação, você poderia especificar um pacote de arquivo em lote final que faz pós-configuração. Qualquer tipo de pacote pode ser preliminar ou final, mas o método de entrega deve ser envio. O método de entrega por envio suportado por diretiva não suporta pacotes preliminares e finais.

Você pode especificar pacotes preliminares e finais quando agendar uma tarefa de distribuição. A página **Pacote de distribuição** da caixa de diálogo **Tarefa agendada - propriedades** tem as opções **Pacote preliminar** e **Pacote final**. Antes de poder clicar uma dessas opções, é necessário ir para a página **Método de entrega** e selecionar um método de entrega. Para isso, clique em **Envio** para o **Tipo de entrega** e clique no **Método de entrega** que você desejar usar.

Para usar a distribuição de vários pacotes em uma tarefa.

1. Crie os pacotes que quiser usar na tarefa.
2. Clique em **Ferramentas > Distribuição > Tarefas agendadas**. Clique no botão **Criar tarefa de distribuição de software** na barra de ferramentas.
3. Na guia **Método de entrega** clique em **Envio** como **Tipo de entrega** e clique no **Método de entrega** que desejar usar.
4. Na guia **Pacote de distribuição**, clique em **Tipo de entrega** e clique no **Pacote de distribuição** que desejar usar.
5. Clique em **Pacote preliminar**, **Pacote principal** ou **Pacote final**, dependendo de quanto você quiser que o pacote seja instalado e clique em **Configurar**.
6. Repita as etapas 4 e 5 para qualquer outro pacote que quiser que seja instalado para esta tarefa. Você só pode ter um pacote em cada estágio e deve sempre ter um **Pacote principal**.
7. Complete a configuração da tarefa e agende-a.

Sobre o download de arquivo

A distribuição de software tem vários métodos para enviar o arquivo para o dispositivo para a instalação. Esses métodos são:

- Obtenção do arquivo do cache de multidifusão
- Obtenção do arquivo de um parceiro
- Download diretamente da fonte remota

Quando um arquivo precisa ser baixado, o agente de distribuição de software do dispositivo, o SDClient, primeiro verifica o cache para determinar se o arquivo está localizado ali. O cache é definido como C:\Arquivos de programa\LANDesk\LDClient\sdmcache ou o caminho é armazenado no "Diretório de cache" na chave de registro de multidifusão:

- HKEY_LOCAL_MACHINE\SOFTWARE\Intel\LANDesk\LDWM\Distribution\Multicast

A estrutura de arquivos no cache será idêntica à estrutura dos arquivos no servidor de web ou de rede. Isso permite a múltiplos pacotes terem arquivos com o mesmo nome e não causar problemas.

Se o arquivo não estiver no cache, em geral, o SDClient tentará descarregar o arquivo de um parceiro na rede. Você pode configurar o método de distribuição para exigir um download de parceiro.

Se o arquivo não puder ser obtido de um parceiro, o SDClient descarregará os arquivos diretamente da fonte UNC ou URL. Você pode configurar o método de entrega de forma que se o arquivo deve ser obtido da fonte, somente um dispositivo no domínio de multidifusão descarregará o arquivo do local da fonte. Na maioria das circunstâncias o download de um compartilhamento UNC requer que este seja um compartilhamento de sessão NULL. Se o arquivo a ser descarregado é baseado em URL, o SDClient o descarregará do site de web.

Em ambos os casos, o SDClient colocará o arquivo no cache de multidifusão (multicast). Após ele ser colocado no cache de multidifusão, o SDClient processa o arquivo baixado.

Quando um arquivo é descarregado no cache, ele permanece ali por vários dias, mas acaba sendo excluído. O tempo que o arquivo permanecerá no cache é controlado pelo método de distribuição usado na distribuição do pacote.

Atualizar hash dos pacotes

Muitos arquivos de pacote são obtidos de parceiros na rede, por isso os arquivos são verificados antes da instalação. A integridade dos arquivos é verificada pela comparação do hash MD5 do arquivo com o hash MD5 gerado no servidor núcleo.

Quando um pacote de distribuição é agendado inicialmente, o Management Suite faz o download de arquivos e calcula os valores de hash associados ao arquivo primário e aos arquivos adicionais utilizados pelo pacote de distribuição. Se o hash armazenado com o pacote não corresponder o valor do hash computado pelo SDClient no dispositivo alvo, o download não será considerado válido.

Se você fizer alguma mudança no pacote fora do Management Suite, por exemplo, uma atualização do conteúdo do pacote, é necessário redefinir o hash, do contrário as tarefas agendadas usando o pacote atualizado falharão.

Para redefinir um hash de pacote

1. Clique em **Ferramentas > Distribuição > Pacotes de distribuição**.
2. No menu de atalho do pacote cujo hash você quer atualizar, clique **Reiniciar hashs de arquivo**. Isso pode levar alguns minutos em pacotes grandes.

Executar a distribuição de pacotes a partir do servidor de origem

A distribuição de software normalmente descarrega arquivos de pacote no cache do dispositivo local e depois instala o pacote a partir do cache. Isso pode não funcionar muito bem se um pacote ou aplicativo contar com os arquivos de instalação em uma estrutura específica de pasta, como, por exemplo, com o instalador do Microsoft Office. Pode também não funcionar se a instalação do aplicativo não usar todos os arquivos de origem para cada instalação.

Nesses casos, faça com que o agente de distribuição de software local rode o arquivo diretamente da origem, independentemente de ser um servidor preferencial ou a origem especificada no pacote. Quando você habilita a execução a partir da origem, a distribuição de software não descarregará arquivos de pacote ao cache local. Também não executará o pacote a partir de um parceiro.

Ao usar a execução da origem com pacotes armazenados nos compartilhamentos de Web, o arquivo primário deve ser um arquivo MSI ou pacote SWD. O arquivo primário pode ser de qualquer tipo com os compartilhamentos UNC.

Para criar um método de entrega que usa executar da origem

1. Clique em **Ferramentas > Métodos de entrega > Utilização da rede**.
2. Clique em **Use executar da origem para distribuir arquivos**.
3. Termine a configuração do método de entrega.

Uso da distribuição de software com pacotes em um sistema de arquivos distribuídos (DFS)

O DFS usa vários servidores para fornecer arquivos disponíveis de um único compartilhamento. O método padrão de detecção de largura de banda da distribuição de software em um cenário DFS usa o servidor raiz para calcular a largura de banda, o que pode não ser o mesmo servidor que fornece o arquivo. A distribuição de software agora fornece uma maneira opcional de calcular a largura de banda. Com esse novo método, a detecção de largura de banda carrega uma pequena parte do arquivo sendo distribuído. Dessa maneira, a distribuição de software calcula a largura de banda a partir do servidor fornecendo o arquivo.

Esse método alternativo de detecção de largura de banda não é habilitado por padrão. Essa opção é ativada no arquivo ntstacfg.in# file na pasta ldlogon do servidor núcleo. Quando tiver atualizado esse arquivo, as mudanças se tornam parte das configurações novas ou atualizadas de agente. É necessário redistribuir a configuração de agente aos dispositivos para que a mudança entre em efeito.

Procure por essa seção no arquivo ntstacfg.in# e faça as mudanças necessárias.

```
; Os seguintes valores de registro controlam a detecção de largura de banda por descarregamento de
arquivo
; altere o valor UseDownloadForBandwidth para 1 para ativar o uso do descarregamento de arquivos para
detecção de largura de banda
; o valor DownloadSize deve ser um valor Hex entre 400 e FFFF(de 1024 a 65535 bytes).
REG1=HKEY_LOCAL_MACHINE,
SOFTWARE\LANDesk\ManagementSuite\WinClient\SoftwareDistribution\UseDownloadForBandwidth, 0, , REG_DWORD
REG2=HKEY_LOCAL_MACHINE, SOFTWARE\LANDesk\ManagementSuite\WinClient\SoftwareDistribution\DownloadSize,
2000, , REG_DWORD
```

Sobre o reinício do ponto de verificação a nível de byte e o controle dinâmica da largura de banda

O Management Suite 8 e as versões posteriores suportam o reinício do ponto de verificação no nível de byte e o controle dinâmico de largura de banda. O reinício do ponto de verificação funciona com as tarefas de distribuição que o SWD copia, em primeiro lugar, para a pasta de cache do dispositivo (por padrão, C:\Arquivos de programas\LANDesk\LDCLIENT\SDMCACHE). Quando uma opção de controle de banda larga é selecionada, os arquivos são copiados primeiro para o cache do dispositivo e o reinício do ponto de verificação permite que as distribuições interrompidas sejam retomadas a partir do ponto onde pararam.

O **Limite dinâmico da largura de banda** especifica que o tráfego de rede que um dispositivo cria tem prioridade sobre o tráfego da distribuição. Essa opção também força um download completo do arquivo para a cache do dispositivo, que também permite o reinício do ponto de verificação ao nível de byte, onde os downloads são retomados de onde pararam, se foram interrompidos. Se você selecionar essa opção e deixar a porcentagem **Largura de banda mínima disponível** com o valor 0, quando o dispositivo iniciar o tráfego da rede, a distribuição retornará cerca de um pacote por segundo até o tráfego parar. O aumento do valor mínimo disponível de largura de banda preserva aproximadamente a quantidade de largura de banda de dispositivo especificada para a distribuição se esta precisar de largura de banda de rede e se houver contenção de largura de banda no dispositivo.

Se estiver instalando ou reparando um pacote SWD ou um pacote MSI, você talvez não queira usar a opção do Limite dinâmico da largura de banda, porque esses tipos de pacote normalmente fazem o download somente dos arquivos de que precisam. Usar o throttling dinâmico de largura de banda, nesse caso, forçaria um download completo do pacote, quando um reparo normalmente requerer somente uma pequena parte do pacote.

Você pode configurar o Limite coletivo da largura de banda de forma que um dispositivo do domínio de multidifusão seja descarregado da fonte remota. Você também pode configurar a quantidade de banda larga usada quando descarregar da fonte. Esse recurso está disponível em todas as versões dos sistemas Windows. Collective bandwidth throttling isn't available on Macintosh systems.

Uso da Multidifusão dirigida com a distribuição de software

A tecnologia Multidifusão dirigida da LANDesk permite distribuir grandes pacotes a muitos usuários em toda a rede com um mínimo de tráfego da rede. Os recursos de Multidifusão dirigida não requerem infra-estrutura adicional de hardware ou software nem reconfigurações de roteadores para a multidifusão de pacotes. Você tem todos os benefícios extraordinários da tecnologia de multidifusão sem nenhuma de suas tradicionais dores de cabeça.

A Multidifusão dirigida é desenvolvida para funcionar com os pacotes de distribuição de software já existentes. Ao usar a Multidifusão dirigida, você poderá distribuir softwares facilmente, mesmo em ambientes WAN com vários saltos e velocidade de conexão baixa (56 k). A Multidifusão dirigida usa HTTP para entrega de um site a um representante de sub-rede. A análise de inventário da Management Suite fornece todas as informações de sub-rede ao serviço de Multidifusão dirigida.

A Multidifusão dirigida fornece benefícios exclusivos que os métodos padrão de "multidifusão" não oferecem. O direcionamento de dispositivos com base em inventário permite enviar um pacote a um grupo selecionado de computadores que atende a critérios específicos por meio de uma multidifusão. A Multidifusão dirigida também é simplificada porque não há necessidade de configurar roteadores para as entregas.

Quando comparada a métodos convencionais de distribuição de software, a Multidifusão dirigida reduz significativamente o tempo e a largura de banda necessários para distribuir pacotes de software. Em vez de enviar um pacote pela rede para cada dispositivo, apenas uma transferência é realizada para cada sub-rede. A economia em largura de banda aumenta à medida que o número de dispositivos em cada sub-rede aumenta.

Você pode ativar a Multidifusão dirigida nas propriedades de método de entrega checando a opção **Usar a Multidifusão para distribuir arquivos** na página **Multidifusão** das propriedades de **Métodos de entrega**. A multidifusão está disponível nos métodos de distribuição suportados, envio de diretiva suportada, envio e multidifusão (somente cache). Por baixo da página de **Utilização de rede** você encontra várias páginas que permitem a configuração de multidifusão.

Quando iniciar uma distribuição usando Multidifusão dirigida, você verá a janela **Distribuição de software de multidifusão**. Essa janela contém informações detalhadas sobre o andamento do processo de distribuição. Para ver mais informações sobre o significado de cada campo, clique no botão **Ajuda** da janela **Distribuição de software de multidifusão**.

Dispositivos Windows e Macintosh OS 10.2 suportam Multidifusão dirigida. Além disso, você pode fazer multidifusão de imagens de distribuição de SO.

Uso de download de parceiro

O download de parceiro é uma opção da Multidifusão dirigida que força os dispositivos alvo a instalarem um pacote da cache local dos dispositivos ou de um parceiro na mesma sub-rede. Essa opção conserva a largura de banda da rede, mas para que a instalação do pacote seja bem-sucedida, o pacote deve estar na cache local ou na cache de um parceiro.

Se você não selecionar a opção **Download de parceiro**, o agente do dispositivo Multidifusão dirigida ainda tentará conservar a largura de banda verificando as seguintes localizações de arquivos de pacotes nesta ordem:

1. Cache local
2. Parceiro na mesma sub-rede
3. Servidor do pacote

Cópia de arquivos para a pasta local de cache de multidifusão

Você tem a opção de copiar um ou mais arquivos para a pasta local de cache de multidifusão utilizando a multidifusão. Essa opção copia um arquivo no cache local do cliente alvo. Ela não instala o arquivo nem executa nenhuma ação com ele. Essa opção é útil para obter arquivos para os representantes de domínio de multidifusão ou para um dispositivo em cada domínio de multidifusão. É possível fazer uma distribuição inicial nos representantes de domínio e depois refazer a distribuição com a opção de download de parceiro para se certificar de que os dispositivos façam o download do pacote somente de um parceiro em sua sub-rede.

Configuração de Multidifusão dirigida

Antes de usar a Multidifusão dirigida, você precisa verificar se os respectivos componentes estão no local correto na sub-rede para a qual você está fazendo a distribuição. A multidifusão dirigida requer agentes do Management Suite e um representante de domínio de multidifusão.

Para especificar manualmente quais computadores serão representantes de domínio de multidifusão:

1. Na tela de rede, clique em **Configuração > Representantes de domínio de Multidifusão**.
2. Adicione representantes de domínio arrastando os computadores que serão representantes da tela de rede para essa categoria.

A Multidifusão dirigida usará o primeiro computador que responder por sub-rede no grupo **Representantes de domínio de Multidifusão**.

Apenas computadores Windows podem ser representantes de domínio de multidifusão. Se você estiver usando a multidifusão para distribuir pacotes a computadores Macintosh, verifique se existe ao menos um computador Windows no domínio de multidifusão para atuar como representante de domínio de computadores Macintosh. Se você tiver apenas alguns computadores Windows em um ambiente onde o Macintosh predomina, é melhor especificar manualmente os representantes de domínio Windows no grupo de Representantes de domínio de multidifusão.

Você pode controlar multidifusões mudando ao deslizadores na página **Usa da largura de banda** sobe a página **Utilização de rede** nas janelas de método de entrega **Envio suportado por diretiva**, **Envio** e **Multidifusão**.

É possível personalizar as opções de Multidifusão dirigida na caixa de diálogo Configurar serviços do Management Suite. Para configurar o serviço de Multidifusão dirigida, clique na guia **Configurar > Serviços > Multidifusão**. Clicar em **Ajuda** na guia para ver mais informações.

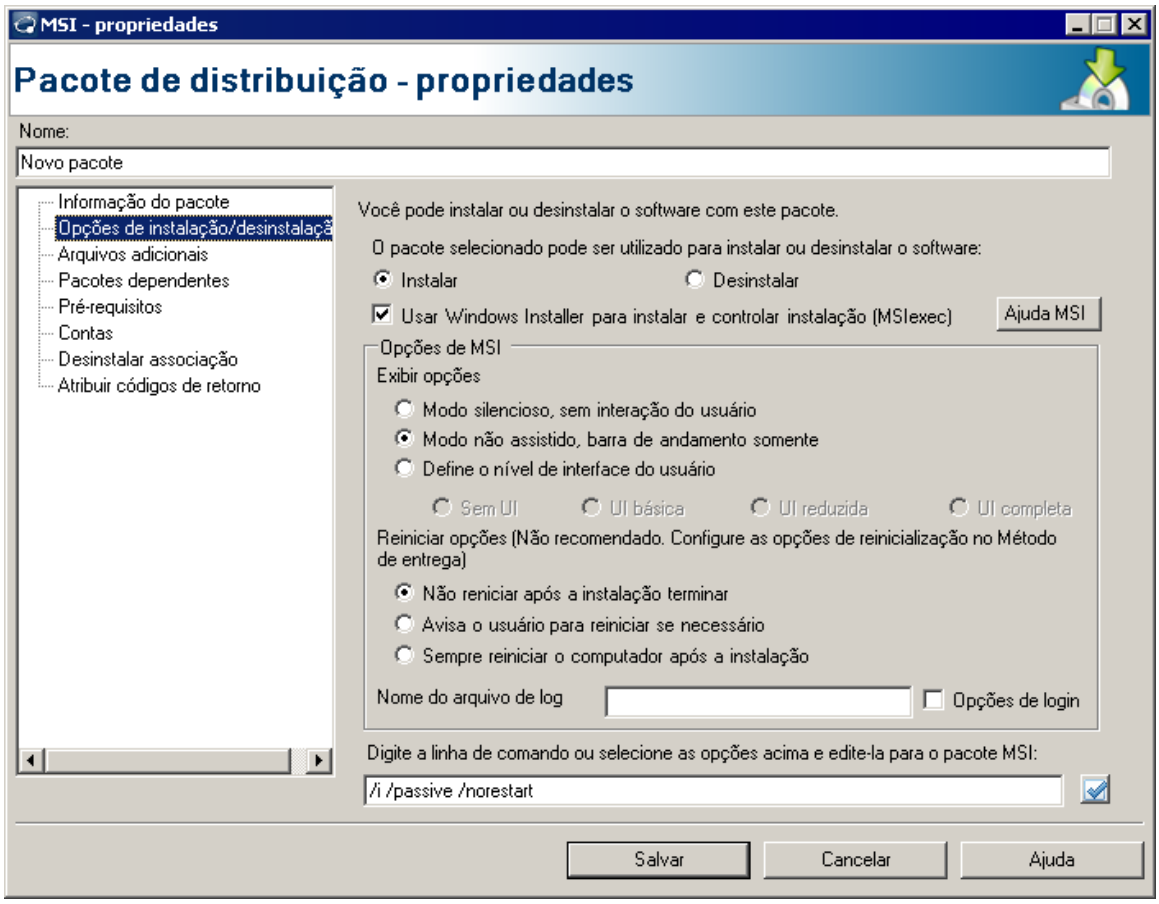
Uso de pacotes de distribuição MSI

O Management Suite suporta a instalação do MSI com relatório de status completo e reconhecimento de pacote MSI. O tipo de pacote de distribuição MSI é o método preferido do Management Suite em termos de distribuição de software. A compreensão dos parâmetros MSI ajudará na configuração dos pacotes MSI e métodos de entrega.

USando os parâmetros de linha de comando MSI com a distribuição de software

Ao instalar um pacote de distribuição MSI, o Management Suite solicita as chamadas MSI API. A instalação do MSI usa dois tipos diferentes de parâmetros de linha de comando:

- Parâmetros de opções
- Parâmetros de referência de propriedades


MSI - propriedades
Pacote de distribuição - propriedades
Nome:
Novo pacote
Informação do pacote
Opções de instalação/desinstalaçã
Arquivos adicionais
Pacotes dependentes
Pré-requisitos
Contas
Desinstalar associação
Atribuir códigos de retorno
Você pode instalar ou desinstalar o software com este pacote.
O pacote selecionado pode ser utilizado para instalar ou desinstalar o software:
Instalar
Desinstalar
Usar Windows Installer para instalar e controlar instalação (MSIexec)
Ajuda MSI
Opções de MSI
Exibir opções
Modo silencioso, sem interação do usuário
Modo não assistido, barra de andamento somente
Define o nível de interface do usuário
Sem UI
UI básica
UI reduzida
UI completa
Reiniciar opções (Não recomendado. Configure as opções de reinicialização no Método de entrega)
Não reiniciar após a instalação terminar
Avisa o usuário para reiniciar se necessário
Sempre reiniciar o computador após a instalação
Nome do arquivo de log
Opções de login
Digite a linha de comando ou selecione as opções acima e edite-la para o pacote MSI:
/i /passive /norestart
Salvar
Cancelar
Ajuda

Parâmetros de opções

Os parâmetros de opção são switches usados pela ferramenta de instalação da Microsoft, Msiexec.exe. Por exemplo, o switch /q switch, é um switch comum para o Msiexec que silencia uma instalação autônoma.

Na caixa de diálogo **Propriedades de distribuição de pacotes**, os parâmetros de opção MSI podem ser inseridos no campo **Linha de comando** da página **Opções de Instalação/Desinstalação**. Clique no botão de marca de verificação próxima do campo para validar a linha de comando. Mais informações sobre as opções Msiexec podem ser encontradas em: http://support.microsoft.com/?kbid=227091.

Parâmetros de referência de propriedades

As referências de propriedade, também conhecidas como propriedades públicas, são específicas ao arquivo MSI. Os parâmetros são passados para os APIs de instalação do MSI diretamente. Eles podem ser usados no campo **Linha de comando** nas **Opções de Instalação/Desinstalação** de um pacote de distribuição MSI.

A sintaxe das referências de propriedade é PROPERTY=VALUE. Uma referência de propriedade comum é a propriedade Transforms. Esta é a propriedade quechama um arquivo .mst (transform). Para obter mais informações sobre os parâmetros de referência de propriedade, consulte: http://support.microsoft.com/?kbid=230781.

As informações nas propriedades públicas do aplicativo podem ser obtidas na documentação da instalação de software, no site oficial do aplicativo ou entrando em contato diretamente com o fornecedor.

Executando silenciosamente um MSI

No Management Suite, a execução silenciosa do MSI é tratada automaticamente na sessão **Opções de instalação/remoção** de um método de entrega. Para executar silenciosamente o MSI, vá para a página **Opções de instalação/desinstalação** para o método desejado de entrega é clique em **Modo silencioso, sem interação do usuário**.

Automatizando uma instalação MSI

Para muitos MSI, o silenciamento dele também automatiza a instalação. Em tais casos, tudo o que você precisa fazer para automatizar uma instalação MSI é selecionar **Modo silencioso, sem interação do usuário** no método de entrega.

Às vezes, uma referência de propriedade é necessária para concluir a instalação. Em tais casos, o instalador do MSI solicitará um valor. Durante a instalação automática, tal solicitação não ocorrerá. A instalação MSI falhará com o erro padrão MSI 1603, Erro fatal durante a instalação. As propriedades públicas solicitadas devem ser atribuídas a um valor no campo **Linha de comando** do pacote de distribuição.

Usando um arquivo transform com uma instalação MSI

Os arquivos de resposta para os MSIs são chamados de arquivos transform e possuem a extensão .mst. Nem todas as instalações MSI precisam de um arquivo transform. Contudo, um arquivo transform pode ser usado se houver muitas referências de propriedades que precisam que seus valores sejam alterados ou atribuídos. É suportado pelo aplicativo, um arquivo de resposta pode ser criado para passar em todos os parâmetros de referência de propriedade.

Se um arquivo transform é solicitado, mas não fornecido durante a instalação, ocorrerá o erro 1603, Erro durante a instalação. Normalmente, o fornecedor do software vendor terá as informações necessárias ou uma ferramenta para criar um arquivo transform para seu MSI específico. Por exemplo, para distribuir o volume de uma versão de licença do Microsoft Office 2003, deve ser usado um arquivo transform. A Microsoft possui uma ferramenta chamada Assistente de Instalação Personalizada que é instalada como parte do Office 2003 Resource Kit. O Office 2003 Resource Kit pode ser obtido por download a partir do seguinte site:

- http://download.microsoft.com/download/0/e/d/0eda9ae6-f5c9-44be-98c7¬ccc3016a296a/ork.exe

Se o fornecedor não tiver as informações necessárias ou a ferramenta, a Microsoft fornece uma ferramenta chamada Orca que pode criar um arquivo transform. Para obter ajuda adicional, consulte o arquivo de ajuda do Orca.

Tratando de reinicializações com uma instalação MSI

O Management Suite trata as reinicializações MSI usando a página **Reinicialização** nas propriedades do método de entrega. O LANDesk aprovará automaticamente os parâmetros REBOOT=REALLYSUPPRESS e /NORESTART quando **Nunca reinicializar** for selecionado no método de entrega.

A opção **Sempre reinicializar** passa o parâmetro /FORCESTART.

Reinicialize somente se necessário permite que o MSI cuide da reinicialização. Se a opção de comentário for ativada, o usuário poderá ser solicitado a respeito de quando reinicializar. É importante saber quais ações personalizadas têm suporte do MSI. O Management Suite não pode evitar uma reinicialização iniciada por uma uma ação personalizada.

Lista de verificação MSI

Se uma distribuição envolve um MSI, siga a seguinte lista de verificação.

- Eu possuo a versão correta dos arquivos de instalação, incluindo o MSI e todos os arquivos adicionais para uma distribuição de licença de voluma.
- Eu possuo as informações do fornecedor do software sobre como automatizar e silenciar a instalação e configuração do software e sobre como tratar as reinicializações.
- Eu sei quais parâmetros de propriedade pública devo passar ao MSI.
- Eu sei se este MSI precisa de um arquivo transform para instalar e por isso, criei um.

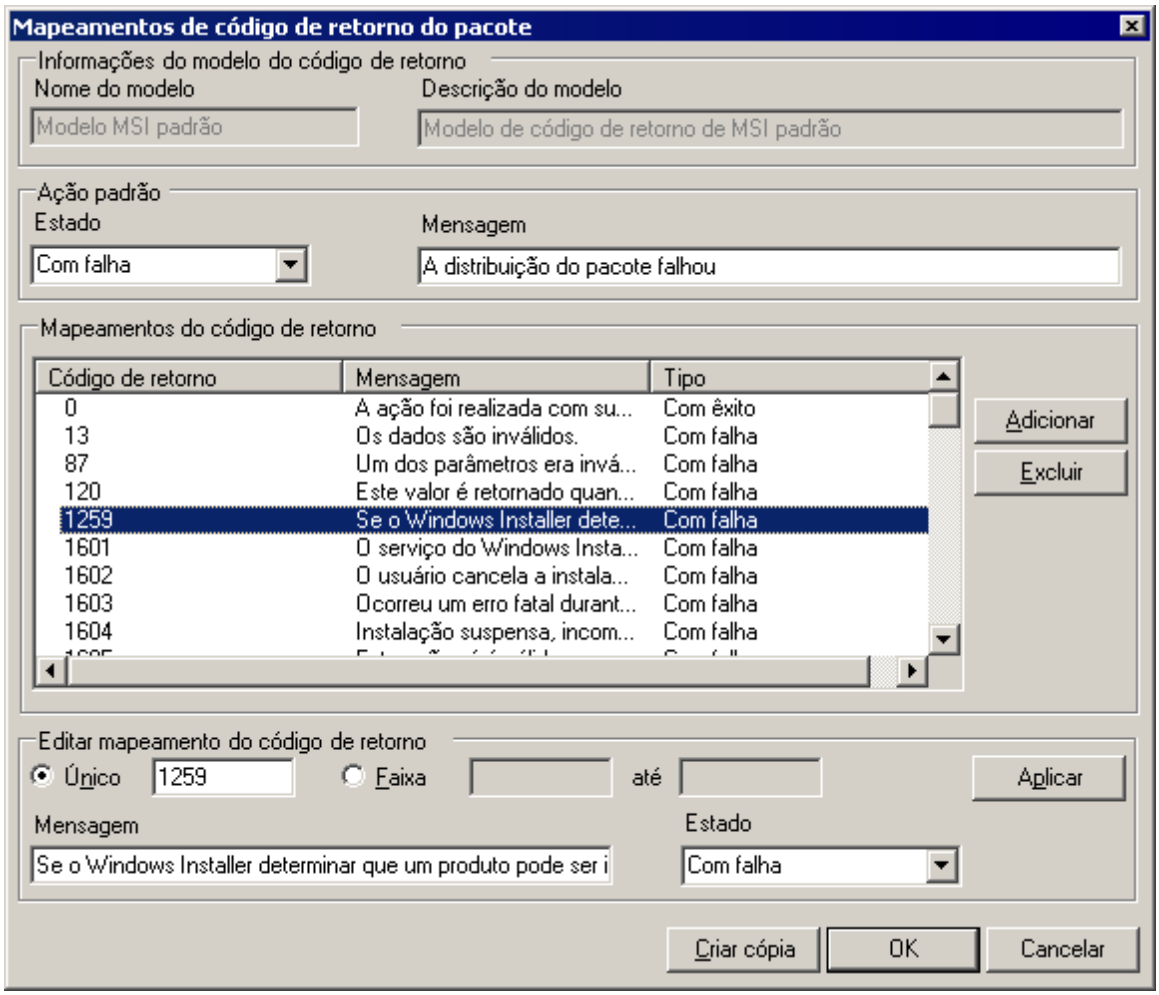
Atribuir códigos de retorno de distribuição

A caixa de diálogo Atribuir códigos de retorno é usada para enviar o status para o servidor núcleo baseado no êxito ou falha da tarefa de distribuição. No passado o Management Suite só lia 0 como sucesso e os outros eram tratados como falha. Isso apresentava problemas aos administradores pois o aplicativo podia ter sido instalado sem erro, entretanto, devido ao fato de que o código de retorno era enviado como um número diferente de 0, o Management Suite indicava falha.

Os fabricantes mantêm listas criadas por desenvolvedores de produto de todos os códigos de retorno possíveis e o resultado específico que os códigos indicam. Agora o Management Suite adiciona o recurso para os administradores consultarem as listas de código de retorno e criar modelos que podem ser associados a pacotes individuais ou múltiplos. Cada código de retorno pode ser designado pelo administrado para indicar êxito ou falha e enviar de volta uma mensagem personalizada indicando resultados específicos da instalação. O Management Suite agora é vendido com um processo de instalador do Windows para os modelos de Office 2003 e Office XP. Para encontrar mais informações nos códigos de retorno inclusos neste modelo visite: http://support.microsoft.com/kb/290158.

Além disso, para usar este recurso com aplicativos de terceiros, os modelos de código de retorno podem também ser criados para aplicações programadas por desenvolvedores internos. O Management Suite fornece um modelo padrão assim como a habilidade de criar novos modelos personalizados; copie o modelo padrão ou os modelos personalizados ou faça modificações a qualquer modelo através do Gerenciador de modelo de código de retorno. Quando os modelos são criados, um modelo específico pode ser associado a um pacote específico na caixa de diálogo Atribuir códigos de retorno através da janela Mapeamentos de código de retorno de pacote. As modificações aos modelos podem também ser feitas deste local.

Os usuário têm a opção de adicionar todos os códigos de retorno possíveis indicando êxito ou falha ou somente adicionar códigos de retorno adicionais que indicam êxigo. No caso que apenas códigos de êxito sejam adicionados, qualquer código de retorno que não for referenciado no modelo é automaticamente mapeado como falha.



Há dois modelos padrão inclusos no Management Suite:

- **Modelo MSI padrão:** Contém acima de 50 mapeamentos que cobrem códigos de retorno MSI padrão.
- **Modelo MSI não padrão:** Contém um mapeamento único para código de retorno 0, "A ação concluíu com êxito". Todos os códigos de erro não zero "Distribuição do pacote falhou".

Um desses modelos está automaticamente atribuído ao pacote de distribuição baseado nesse tipo. Você pode mudar o mapeamento do modelo nas propriedades de um pacote de distribuição.

Atribuir códigos de retorno de distribuição

A caixa de diálogo Atribuir códigos de retorno é usada para enviar o status para o servidor núcleo baseado no êxito ou falha da tarefa de distribuição.

Os usuário têm a opção de adicionar todos os códigos de retorno possíveis indicando êxito ou falha ou somente adicionar códigos de retorno adicionais que indicam êxigo. No caso que apenas códigos de êxito sejam adicionados, qualquer código de retorno que não for referenciado no modelo é automaticamente mapeado como falha.

Para usar o Gerenciador de modelo de código de retorno

1. Clique em **Ferramentas > Distribuição > Pacotes de distribuição**.
2. Na barra de ferramentas **Pacotes de distribuição**, clique em **Gerenciador de modelo de código de retorno**.
3. No diálogo **Gerenciador de modelo de código de retorno**, clique em **Adicionar, Modificar, Excluir, Importar** ou **Exportar**.
4. Clique em **Salvar**.

Para adicionar um novo modelo de mapeamento de código de retorno

1. Clique em **Ferramentas > Distribuição > Pacotes de distribuição**.
2. Na barra de ferramentas **Pacotes de distribuição**, clique em **Gerenciador de modelo de código de retorno**.
3. No diálogo **Gerenciador de modelo de código de retorno**, clique em **Adicionar**.
4. Digite um **Nome de modelo** e a **Descrição do modelo**.
5. Selecione um **Tipo de filtro de modelo**.
6. Clique em **OK**.
7. Se quiser mudar a mensagem padrão para êxito ou falha, selecione um **Estado** na caixa de diálogo **Mapeamentos de código de retorno de pacote**, e insira a **Mensagem** correspondente ao estado.
8. Adicione um novo mapeamento clicando em **Adicionar**.
9. Na parte inferior da caixa de diálogo, digite o código de retorno numérico ou a faixa do código de retorno.
10. Digite a **Mensagem** e selecione um **Estado**.
11. Repita os passos de 8 a 10 se necessário.
12. Clique em **OK**. O seu novo modelo aparece nesta lista.

Para aplicar o mapeamento de código de retorno a um pacote de distribuição

1. Clique em **Ferramentas > Distribuição > Pacotes de distribuição**.
2. Clique duas vezes no pacote que deseja modificar.
3. Na árvore de propriedades do pacote, clique em **Atribuir códigos de retorno**.
4. Clique no modelo de códigode retorno que deseja aplicar.
5. Clique em **Atribuir**.
6. Clique em **Salvar**.

Exportar e importar modelos de código de retorno de distribuição

Os modelos de código de retorno são armazenados no banco de dados núcleo, mas você pode exportar modelos para um arquivo XML e importá-los para outros servidores. Se um pacote de distribuição estiver sendo sincronizado através da sincronização do núcleo, seu modelo de código de retorno é parte dos dados de sincronização.

Para exportar um modelo de código de retorno

1. Clique em **Ferramentas > Distribuição > Pacotes de distribuição**.
2. Na barra de ferramentas **Pacotes de distribuição**, clique em **Gerenciador de modelo de código de retorno**.
3. Clique no modelo que quiser exportar.
4. Clique em **Exportar**.
5. Procure um caminho e digite um **Nome de arquivo**.
6. Clique em **Salvar**.

Para importar um modelo de código de retorno

1. Clique em **Ferramentas > Distribuição > Pacotes de distribuição**.
2. Na barra de ferramentas **Pacotes de distribuição**, clique em **Gerenciador de modelo de código de retorno**.
3. Clique em **Importar**.
4. Procure um arquivo XML que contenha um modelo exportado.
5. Clique em **Abrir**.

Uso do portal de distribuição de software

O acesso à janela Portal de distribuição de software é feito através do Gerenciador de desktop nos dispositivos gerenciados. O portal contém todas as tarefas de pacotes de distribuição de software que foram distribuídas usando um método de entrega baseado em diretiva.

Ao abrir o portal, ele pede para que aguarde enquanto sincroniza-se com o servidor de diretiva para atualizar a lista de aplicativos. Durante esse tempo a sincronização de diretiva está sendo executada e descarregando novas diretivas. As diretivas necessárias não são mostradas na janela Portal de distribuição de software e inicia a instalação automaticamente (a menos que sejam pospostas por um usuário final). As outras tarefas sãomostradas na janela Portal de distribuição de software.

O dispositivo gerenciado inclui um serviço de invocador de diretiva que examina diretivas que são descarregadas. As tarefas de diretiva são armazenadas em um banco de dados pequeno ao serem obtidas. O serviço invocador monitora esse banco de dados e atualiza o status de diretivas conforme elas mudam de um estado para outro. Ele lê também o status das diretivas para determinar se há necessidade de realizar uma instalação. O invocador não instala pacotes. Ele chama o agente de distribuição de software (sdclient.exe), o qual faz a instalação.

Além da atualização da diretiva que ocorre quando um usuário abre o Portal de distribuição de software, essas opções de configuração de agente também afetam os intervalos de atualização de diretiva. Uma atualização ocorre:

- No login, se a opção **Quando o usuário fizer logon** for selecionada.
- Quando o endereço IP de um usuário muda se a opção **Quando o endereço IP mudar** for selecionada.
- No intervalo do planejador local que você especificar quando clicar no botão **Mudar configurações**. Por padrão, os dispositivos gerenciados usam o planejador local uma vez por dia para obter as atualizações de diretivas.

Você pode mudar essas configurações de atualização de diretiva na página **Distribuição de software > Opções de diretiva** do diálogo de configuração de agente.

Distribuição de software para dispositivos Linux

Após ter distribuído os agentes Linux, você pode distribuir software para os dispositivos Linux. A distribuição de agentes Linux inicial usa uma conexão SSH. Uma vez instalados os agentes, o servidor núcleo usa o agente LANDesk padrão para comunicar com o servidor Linux e transferir arquivos. Para distribuir software em um dispositivo Linux, é necessário ter privilégios de administrador.

Só é possível distribuir RPMs para dispositivos Linux. Os agentes Linux instalarão automaticamente cada RPM distribuído. O RPM em si não é armazenado no servidor após a instalação. Você pode instalar e desinstalar o RPM que especificar usando a distribuição de software. Você só pode usar métodos de entrega por envio com a distribuição de software Linux. Para a distribuição de software Linux, as configurações no método de entrega por envio são ignoradas; portanto não importa qual método de entrega por envio foi selecionado ou quais são as configurações escolhidas.

A distribuição segue este processo:

1. O servidor núcleo conecta-se ao dispositivo Linux através do agente LANDesk padrão
2. O dispositivo faz o download do pacote
3. O dispositivo executa um script de shell que usa comandos RPM para instalar o pacote RPM
4. O dispositivo envia o status de volta ao servidor núcleo.

É possível armazenar RPMs Linux em compartilhamentos HTTP. A distribuição de software Linux não suporta os compartilhamentos de arquivo UNC. Para compartilhamentos HTTP, certifique-se de que ativou a pesquisa no diretório para o compartilhamento. Se desejar usar um compartilhamento HTTP em um dispositivo Windows que não seja o núcleo, será necessário configurar o IIS com o tipo MIME correto para arquivos RPM. Caso contrário, o tipo MIME padrão usado pelo IIS fará com que o RPM falhe ao fazer o download do arquivo.

Para configurar o tipo MIME RPM em dispositivos Windows

1. No **Painel de controle** do Windows, abra o **Gerenciador de serviços de Internet**.
2. Navegue para a pasta que contém seus arquivos de distribuição. No menu de atalho desse folder, clique em **Propriedades**.
3. Na guia **Cabeçalhos HTTP**, clique no botão **Tipos de arquivo**.
4. Clique em **Novo tipo**.
5. Para a **Extensão associada** , digite **rpm**. Observe que rpm deve ser digitado em minúsculas.
6. Para o **Tipo de conteúdo**, digite texto/simples.
7. Clique em **OK** para sair das caixas de diálogo.

Após armazenar os arquivos no compartilhamento de pacote, crie um novo pacote de distribuição Linux na janela **Distribuição de pacotes**, associe-o ao método de entrega que desejar e agende a entrega.

Dependências do software Linux

Ao clicar em **Salvar** na caixa de diálogo **Distribuição de propriedades do pacote** de um pacote Linux, a distribuição do software analisa o RPM primário e os RPMs dependentes selecionados para as dependências requeridas pelos RPMs. Essas dependências aparecem na caixa de diálogo **Bibliotecas ausentes**. A seleção de uma dependência nessa caixa de diálogo faz com que a distribuição de software não o avise novamente sobre a mesma. Você pode checar as dependências que tem certeza estarem instaladas nos dispositivos gerenciados. Essa caixa de diálogo serve somente como informação. Se estiver faltando uma dependência em um dispositivo alvo e você não a incluiu como pacote dependente, o RPM provavelmente não irá instalar com êxito.

Solução de problemas de falhas de distribuição

A distribuição de software permite que você distribua pacotes para um grande número de dispositivos de uma só vez. Se houver um problema com o pacote ou se o software sendo distribuído entrar em conflito com o software existente, você poderá causar problemas a milhares de dispositivos de uma só vez. Ao planejar uma distribuição usando a distribuição de software, tenha cuidado para não sobrecarregar a help desk.

Antes de distribuir um novo pacote, teste-o em alguns sistemas de teste. O ideal é que esses sistemas de teste incluam todos os sistemas operacionais e aplicativos que são usados no seu ambiente. Após o pacote ser distribuído, confirme se todos os sistemas e aplicativos ainda estão funcionando como esperado.

Após o pacote ser validado nos sistemas de teste, faça uma distribuição limitada. Selecione um número pequeno de dispositivos no seu ambiente. Ao decidir quantos dispositivos selecionar, a regra geral é não selecionar mais dispositivos que a sua help desk pode suportar. Quando o pacote for distribuído para esses dispositivos, não toque no software por alguns dias para ver se os usuários encontram problemas.

Após a distribuição inicial você pode começar a distribuir o software para outros dispositivos na empresa. A velocidade na qual essa distribuição ocorre deve ser baseada na variedade de dispositivos que empresa possui e na quantidade de carga que o help desk pode suportar.

Para obter mais informações, leia este artigo da comunidade sobre solução de problemas na distribuição de softwares: http://community.landesk.com/support/docs/DOC-5096.

Processar scripts personalizados de distribuição de softwares

Scripts personalizados que controlam tarefas agendadas (**Ferramentas > Distribuição > Tarefas agendadas**) são processados em três seções:

- **Pré-computador:** A seção Pré-computador do script personalizado é processada primeiro e isso ocorre apenas uma vez no início da tarefa. Use esta seção para as tarefas que não têm dispositivos alvo e/ou para Multidifusão dirigida. Durante a seção Pré-computador do script, apenas comandos locais, LOCxxx, devem ser usados.
- **Máquina:** Os comandos nesta seção do script são executados em seguida e apenas uma vez por dispositivo alvo. Esses comandos podem usar os comandos de execução remotos ou locais e são principalmente usados para execução remota de SDCLIENT.EXE. Para que os comandos nessa seção de script possam ser executados, o agente SWD deve ser instalado preliminarmente nos dispositivos alvo.

- **Pós-computador:** Essa seção é processada por último e, novamente, apenas uma vez depois que todos os dispositivos tiverem sido processados. A distribuição de software não adiciona comandos a essa seção e ela oferece suporte apenas aos comandos locais, LOCxxx. Os comandos nessa seção não serão processados se os dispositivos na tarefa não puderem executá-los. O script InventoryScanner.ini que vem com o Management Suite contém detalhes sobre os comandos de script.

Comandos de scripts personalizados

Os scripts personalizados suportam vários comandos locais e remotos:

- **LOCEXEC:** Local execute (Execução local), este comando é usado para executar um aplicativo no dispositivo local, que é sempre o servidor núcleo.
- **LOCDEL:** Local deletion (Exclusão local), exclui arquivos em um dispositivo local.
- **LOCMKDIR:** A pasta Local make (Criação de pasta local) cria uma pasta no dispositivo local.
- **LOCRD:** A Local remove folder (Remoção de pasta local), esse comando é usado para remover uma pasta no dispositivo local.
- **REMCOPY:** Remote copy (Cópia remota), copia um arquivo do dispositivo local para um computador remoto.
- **REMEXEC:** Remote execution (Execução remota), executa um aplicativo no dispositivo remoto especificado
- **REMDEL:** Remote deletion (Exclusão remota), exclui arquivos em um dispositivo remoto.
- **REMMKDIR:** Remote make folder (Criação de pasta remoto), este comando cria uma pasta no dispositivo remoto.
- **REMRD:** Remote remove folder (Remoção remota de pasta), este comando exclui uma pasta no dispositivo remoto.

HTTP e caminho UNC em scripts

Estes são exemplos de arquivos .ini de distribuição de software que refletem as diferenças entre arquivos de script com caminhos HTTP e UNC.

Arquivo de script com caminho HTTP:

```
; Este arquivo foi gerado pelo Gerenciador de Desktop
[COMPUTADORES]
REMEXEC0=C:\Program Files\LANDesk\LDClient\sdclient.exe -p=http://<web server>/packages/test package.exe
-g={6DD454C0-11D3A0D1-a000B3B5-9BACBBC99CFC6D-9CE3504801A0D4B2FZ0829F08} -Ac -Ab
```

Arquivo de script com caminho UNC:

```
; Este arquivo foi gerado pelo Gerenciador de Desktop
[COMPUTADORES]
REMEXEC0=C:\Arquivos de programas\LANDesk\LDClient\sdclient.exe -p=\\sample_core\onefile\test
package.exe -g={6DD454C0-11D3A0D1-a000B3B5-9BACBBC99CFC6D-9CE3504801A0D4B2FZ0829F08} -Ac -Ab
```

Observe que ambos os arquivos .ini têm elementos semelhantes. Na seção COMPUTADORES, a opção -P designa o caminho no qual o dispositivo fará o download do pacote de software. No exemplo HTTP, o caminho é http://<servidor web>/packages/test package.exe.

A próxima opção é a -G, que corresponde ao GUID, um identificador de número exclusivo para cada pacote. Esse identificador de número é gerado pelo Package Builder e ajuda a evitar confusão entre pacotes com nomes semelhantes durante a instalação.

Guia de script para arquivos de scripts de distribuição (.ini)

Você não precisa usar a janela **Criar script de distribuição de software** para criar o arquivo de script de implantação. Um arquivo de distribuição é um arquivo .ini contendo as configurações que o dispositivo deve usar para a instalação de um pacote. Se preferir, crie seus próprios arquivos de distribuição em um editor de texto, por exemplo, usando o Bloco de notas.

Um arquivo de script .ini de distribuição de software contém estes componentes:

```
[COMPUTADORES]
REMEXEC0=C:\Program Files\LANDesk\LDClient\sdclient.exe
/p="http://computer_name/95Packages/Acro32_95.exe"
/g={281B46C0-11D3766F-a0008bab-F9751AC966F808-66E3BC2DF01A0D4B2F88670DE4}
/Ac
/N
```

Parâmetros de comando REMEXEC0

Os parâmetros do comando REMEXEC0 foram colocados em linhas separadas para tornar os componentes mais visíveis. Quando colocado em um arquivo .ini, o comando precisa estar em uma linha.

REMEXEC0 é o comando Execução remota. Se quiser usar mais de um comando REMEXEC0 em um único arquivo de script, incremente o comando toda vez que ele for usado. Por exemplo, se usar três chamadas para o comando REMEXEC em um único arquivo .ini, elas deverão ser REMEXEC0, REMEXEC1 e REMEXEC2. Esses comandos não precisam incrementar se estiverem em arquivos separados.

O parâmetro C:\Program Files\LANDesk\LDClient é o caminho correto para o agente SWD.

Códigos de erro da Distribuição de software

Para obter mais informações gerais sobre a solução de problemas de softwares, veja esta página na Comunidade de usuários da LANDesk:

- http://community.landesk.com/support/docs/DOC-5096

No console, o painel direito na janela **Tarefas agendadas** mostra o status da tarefa. Se clicar em Falhou na tarefa, você pode ver dispositivos que falharam o trabalho e as mensagens e logs resultantes. O status e os erros são registrados nos seguintes arquivos:

- Se o erro tiver ocorrido durante a tentativa de acesso ao pacote, ele será registrado no arquivo AICLIENT.LOG.
- Se o erro tiver ocorrido durante o processamento do pacote (por exemplo, ao copiar os arquivos), ele será registrado no arquivo INST32.LOG.
- O arquivo SDCLIENT.LOG contém informações gerais de resumo sobre cada solicitação de instalação recebida do servidor núcleo.

Esses arquivos de log são armazenados em cada dispositivo.

Opções da linha de comando SDCLIENT.EXE de distribuição de softwares

A distribuição de software é facilitada por um script de implantação. O SDCLIENT.EXE gerencia os pacotes usando os switches de linha de comandos do arquivo de script que são passados ao aplicativo.

Para obter mais informações, leia este artigo da comunidade sobre switches da linha de comando do SDCLIENT.EXE: http://community.landesk.com/support/docs/DOC-13759.

Ajuda da distribuição de software

Uso da caixa de diálogo Pacote de distribuição

A caixa de diálogo **Pacote de distribuição** (**Ferramentas > Distribuição > Pacote de distribuição**) armazena informações no banco de dados, que descrevem o pacote que você deseja distribuir. Os dados contêm as configurações necessárias para se instalar um pacote de software específico, por exemplo, o nome do pacote, quaisquer dependências ou pré-requisitos, opções de instalação etc. Após criadas, tais informações constituem o que chamamos de "pacote de distribuição".

Antes de utilizar esta caixa de diálogo, coloque o pacote no seu servidor de distribuição. Você precisará navegar até o pacote e fornecer informações sobre quaisquer arquivos adicionais ou pré-requisitos do pacote. Uma vez criado o pacote de distribuição, você pode associá-lo a um método de entrega (**Ferramentas > Distribuição > Métodos de entrega**) para distribuí-lo a dispositivos.

Sobre a página Informações do pacote

Use esta página para digitar o nome do pacote e o arquivo primário do seu pacote. Se seu pacote contiver um único arquivo, adicione-o aqui. Se seu pacote contiver vários arquivos, adicione o arquivo principal do seu pacote, por exemplo, o arquivo que inicia a instalação. Você pode adicionar arquivos de suporte adicionais na página **Arquivos adicionais**.

Para usar o localizador de arquivos, digite o caminho de um arquivo ou de um compartilhamento da Web na caixa próxima ao botão **Ir**. Ao clicar em **Ir**, o destino especificado na caixa **Arquivo principal** é exibido. Continue a navegar a partir daí. Ao encontrar o arquivo, clique duas vezes no arquivo para especificá-lo como o arquivo principal. Isto adiciona o nome do arquivo ao caminho do pacote próximo ao botão Ir.

- **Nome:** O nome que for digitado aqui aparece nas árvores e caixas de diálogos de **Pacotes de distribuição** e **Métodos de entrega**. Use um nome descritivo, mas não muito longo, já que você terá de rolar a tela para poder ver descrições longas.
- **Descrição para mostrar ao usuários finais no download:** A descrição que for digitada aqui aparece nas janelas **Pacotes de distribuição** e **Métodos de entrega** e no Portal de distribuição de software.
- **Arquivo principal:** O arquivo principal no pacote.
- **Ir:** Inicia a pesquisa no caminho digitado próximo ao botão Ir.
- **Para cima:** Vai para o nível de pastas acima do nível atual onde você está pesquisando.

Usando variáveis de ambiente

Não há suporte, no Management Suite, para a colocação da variável do ambiente diretamente no caminho do pacote, embora a expansão ainda funcione com scripts personalizados previamente criados. Para oferecer suporte às variáveis de ambiente da nova arquitetura da SWD, o valor do registro "PreferredPackageServer" deve ser configurado de acordo com a variável de ambiente a ser utilizada. Esta variável de ambiente será então expandida para definir o servidor de onde o pacote deve ser recuperado.

Sobre a página Opções de instalação/desinstalação

Use essa página para especificar o tipo de pacote. Você tem várias opções, dependendo do pacote que estiver distribuindo. Nem todos os tipos de pacotes têm essas opções.

- **Instalar:** Especifica que você deseja usar um pacote de instalação para instalar o software.
- **Desinstalar:** Especifica que você deseja usar um pacote de instalação para remover o software. Quando esse sinalizador for definido, o script removerá tudo o que tiver sido instalado com o script de instalação.
- **Linha de comandos:** (Não está disponível para pacotes SWD, Macintosh, ou Linux) A linha de comandos que você deseja que passada para o arquivo principal especificado. A distribuição de software adiciona automaticamente os parâmetros básicos para o tipo de pacote que estiver sendo distribuindo.

Opções de instalação/desinstalação do MSI

Os pacotes de distribuição MSI têm opções adicionais de instalação/desinstalação quando você seleciona **Usar o Instalador do Windows para instalar e controlar a instalação (MSIexec)**.

- Opções de tela:
  - **Modo silencioso, sem interação do usuário:** Executa a instalação sem notificação no dispositivo gerenciado (instalação silenciosa).
  - **Modo não assistido, barra de andamento apenas:** Mostra apenas uma barra de andamento durante a instalação sem concelamento ou opções de adiamento.

  • Configura o nível de interface do usuário:

  - **Sem interface de usuário:** Executa uma instalação silenciosa completamente.
  - **Interface de usuário básica:** Exibe uma janela de tamanho inteiro com uma barra de andamento e um botão Cancelar. Aparece uma caixa de mensagem no fim da instalação. Se você cancelar a instalação, não será exibida uma caixa de mensagem.
  - **Interface de usuário reduzida:** Mostra uma caixa de mensagem no fim da instalação.
  - **UI completa:** Exibe uma janela de tamanho inteiro com uma barra de andamento e um botão Cancelar. Aparece uma caixa de mensagem no fim da instalação.
- Opções de reinício:
  - **Não reinicie após a instalação terminar:** Não executa uma reinicialização mesmo se uma instalação tiver sido programado para isso.
  - **Avisar o usuário para reiniciar se necessário:** Avisa o usuário para reinicializar se o arquivo de instalação exigir.
  - **Sempre reiniciar o computador após a instalação:** Executa uma reinicialização após a instalação terminar.
- **Nome do arquivo de log:** Especifica o local e o nome do arquivo para armazenar um arquivo de log do Instalador do Windows com base nos resultados da instalação após a conclusão.
- **Opções de log:** Habilita a criação do arquivo de log após o local ter sido especificado.

- **Inserir uma linha de comando ou selecionar as opções acima e editar linha de comando para pacote MSI:** (Não está disponível para pacotes SWD) Mostra a linha de comando que será passada para o arquivo primário especificado. A distribuição de software adiciona automaticamente os parâmetros básicos aqui para mudar os comportamentos padrão. Os campos da linha de comando podem também acessar valores de inventário usando macros do banco de dados. Especifique o item de inventário encapsulado no símbolo. Por exemplo:

  %Nome_Dispositivo.Computer%

  Mostra o nome do dispositivo com o sublinhado usado no lugar do espaço e o computador no topo da árvore do inventário.

Sobre a página de opções de Lote

As opções nesta página são aplicáveis à pacotes que usem arquivos de scripts ou lotes. Por padrão, os pacotes são executados em modo de 32 bits, o que significa:

- Se um aplicativo 32 bits acessar os valores de registro em HKEY_LOCAL_MACHINE\SOFTWARE, estará, na verdade, acessando os valores em HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node.
- Se um aplicativo de 32 bits executar um programa localizado em c:\windows\system32, estará, de fato, executando uma versão de 32 bits do aplicativo do C:\Windows\SysWOW64. O que inclui: cmd.exe, cscript.exe, wscript.exe e outros.

Se você selecionar **Executar como aplicativo de 64 bits no Windows de 64bits**, os arquivos de scripts e lote irão:

- Leia e escreva em HKEY_LOCAL_MACHINE\SOFTWARE em vez de HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node
- Eles executarão aplicativos de 64 bits do System32 em vez de aplicativos de 32 bits (em c:\windows\SysWOW64)

Para obter mais informações da Microsoft sobre a execução de aplicativos de 32 bits em ambiente de 64 bits, consulte esta página do MSDN:

- http://msdn.microsoft.com/en-us/library/aa384249(VS.85).aspx

Sobre a página Opções da fila de clientes

Use a página de Opções da fila de clientes para configurar como você quer que os trabalhos simultâneos de distribuição sejam tratados.

A fila de clientes permite que trabalhos múltiplos simultâneos sejam processados por cada cliente na ordem que são recebidos, com prioridade para os trabalhos do tipo 'push'.

Os trabalhos ainda são processados um por vez, mas a fila permite que vários trabalhos sejam executados ao mesmo tempo ao invés de causar uma falha no novos trabalhos se um trabalho já estiver em execução.

- **Desabilitar enfileiramento de clientes para este pacote:** Desabilita o enfileiramento no pacote atual. Se um dispositivo recebe um trabalho enquanto outros trabalhos estiverem ativos, o trabalho falhará.

Sobre a página Arquivos adicionais

Se seu pacote contiver vários arquivos, adicione-os nesta página. Para usar o localizador de arquivos, digite um caminho de arquivo ou de compartilhamento da Web na caixa próxima ao botão Ir. Ao clicar em Ir, o destino especificado na caixa **Arquivos disponíveis** é exibido. Continue a navegar a partir daí. Selecione os arquivos na caixa **Arquivos disponíveis** e clique em **>>** para adicioná-los à lista **Arquivos adicionais**. Isto adicionará os arquivos ao pacote.

- **Detecção automática:** Esta opção está disponível para pacotes MSI. Ela analisa o arquivo MSI principal à procura de referências a arquivos externos e automaticamente adiciona esses arquivos.
- **Setas:** Estas setas adicionam ou removem os arquivos selecionados da lista **Arquivos adicionais**.
- **Botão Ir:** Inicia a pesquisa no caminho digitado próximo ao botão Ir.
- **Botão Para cima:** Vai para o nível de pastas acima do nível atual onde você está pesquisando.

Usando a página Pacotes dependentes

Pacotes dependentes são aqueles que já devem se encontrar no dispositivo para que o pacote que você está configurando possa ser instalado. Se eles não se encontrarem no dispositivo, os pacotes dependentes serão instalados automaticamente. Pacotes MSI e SWD são detectados automaticamente através das chaves do registro apropriadas no dispositivo. Para os outros tipos de pacote, o método de detecção do pacote depende do que você selecionar na página Detecção.

Se você adicionar um pacote existente com uma dependência como pacote dependente para o pacote que estiver criando, essa dependência também será adicionada ao novo pacote.

- **Pacotes disponíveis:** contém os pacotes públicos que você criou usando a janela **Pacotes de distribuição**. Somente pacotes públicos podem ser dependentes. Selecione os pacotes que deseja configurar como dependentes e clique em **>>**.
- **Pacotes dependentes::** Lista os pacotes que você especificou como dependentes.
- **Setas:** Estas setas adicionam ou removem os arquivos selecionados da lista **Arquivos adicionais**.
- Botões **Para cima** e **Para baixo**: Os pacotes dependentes são aplicados para aparecerem na lista **Pacotes dependentes**. Use os botões **Para cima** e **Para baixo** para mudar a ordem do pacote dependente.

Dependências do software Linux

Ao clicar em **Salvar** na caixa de diálogo **Distribuição de propriedades do pacote** de um pacote Linux, a distribuição do software analisa o RPM primário e os RPMs dependentes selecionados para as dependências requeridas pelos RPMs. Essas dependências aparecem na caixa de diálogo **Bibliotecas ausentes**. A seleção de uma dependência nessa caixa de diálogo faz com que a distribuição de software não o avise novamente sobre a mesma. Você pode checar as dependências que tem certeza estarem instaladas nos dispositivos gerenciados. Essa caixa de diálogo serve somente como informação. Se estiver faltando uma dependência em um dispositivo alvo e você não a incluiu como pacote dependente, o RPM provavelmente não irá instalar com êxito.

Usando a página Pré-requisitos

A página Pré-requisitos lhe permite especificar os pré-requisitos para a instalação do pacote. Você pode fazer isto através de uma consulta ou através de um programa/arquivo adicional que é executado nos dispositivos, e que retorna um código de nível de erro. Um código diferente de zero não permitirá que o pacote seja instalado .

Os pré-requisitos são executados nos dispositivos na lista de alvos. Se um dispositivo na lista de alvos não tem o pré-requisito, o pacote não é instalado nele. Os detalhes da falha estão no log da tarefa de distribuição.

Pré-requisitos são especificamente úteis em organizações onde uma pessoa cria pacotes e outra pessoa é responsável por distribuí-los. O distribuidor pode não saber sobre os requisitos de sistema do pacote, que são de conhecimento do criador do pacote. Em casos como este, o criador do pacote pode criar uma consulta que inclua os requisitos do pacote, como o sistema operacional ou a quantidade de memória.

Para a opção de arquivos adicionais, é possível selecionar um arquivo que esteja na lista de arquivos adicionais do pacote. Você então poderá especificar uma linha de comandos na qual você deseja que o arquivo seja executado.

- **Escolha uma consulta:** Escolha uma consulta existente para filtrar os dispositivos alvo. Clique também em **Criar consulta** para criar uma nova consulta.
- **Executar o arquivo adicional:** Se desejar executar um arquivo nos dispositivos, marque esta opção.
- **Escolher um arquivo adicional:** Digite o arquivo a ser executado nos dispositivos. Este arquivo é executado antes de quaisquer outros arquivos de pacotes.
- **Linha de comandos:** Se o arquivo que você especificar precisar de uma linha de comandos, digite-a aqui.

Uso da página Detecção

Use a página Detecção para configurar o modo como as distribuições detectam se um pacote já foi distribuído. A página Detecção está disponível apenas para pacotes executáveis e pacotes de Aplicativo virtualizado. Se forem satisfeitos um ou mais critérios, o pacote é impedido de ser instalado.

Os seguintes métodos de detecção podem ser usados:

- **Detectar por:** Determina se um pacote já está instalado, por atender a um destes critérios:
  - O arquivo existe
  - Versão do arquivo
  - Tamanho do arquivo e/ou soma de comprovação:
  - Data do arquivo
  - A chave do registro existe
  - A chave do registro existe
  - Comparando o valor do registro
- **Caminho do arquivo:** Especifica o local e o nome do item a detectar.
- **Procurar o arquivo recursivamente:** Pesquisa em cascata pelos subdiretórios a partir do diretório especificado no campo **Caminho do arquivo**.

Múltiplos critérios podem ser adicionados especificando-se os critérios e clicando no botão **Adicionar**.

Os pacotes MSI e SWD distribuem GUIDs com suas instalações. Eles são usados para detectar se um pacote já está instalado. A opção de detecção não está disponível nesses tipos de pacote.

Usando a página de Contas

Use a página de Contas para selecionar o tipo de conta de usuário para usar na distribuição do pacote.

- **Conta LocalSystem:** A conta do dispositivo.
- **Conta atual do usuário:** A conta do usuário atual. Um usuário deve estar conectado no dispositivo ou a tarefa de distribuição do pacote falhará.

- **Executar como usuário especificado:** A conta de um usuário que você especificar. Você deve fornecer um **Domínio\nome de usuário** e **Senha** para o usuário que você quer usar.

Usando a página Configurações do tempo limite

Use a página Configurações do tempo limite para definir um limite de tempo para a instalação.

- **Habilite o limite de tempo de instalação do pacote:** Quando selecionado, o número de horas que você quer que a instalação dure. Se o pacote não for instalado até que o tempo limite seja atingido, o trabalho será considerado malsucedido.

Usando a página Associação de desinstalação

Use a página Associação de desinstalação para associar a desinstalação de um pacote a diretiva de distribuição de software de um pacote. Isso desinstalará automaticamente o software do cliente quando a máquina ou o usuário for removido da lista de alvo ou consulta. **NOTA:** A desinstalação de pacotes é usada somente com a distribuição com base nas diretivas.

- **Tipo:** Selecione o tipo de pacote que deseja usar para desinstalar o pacote. A lista de pacotes de distribuição disponíveis mostrará somente os pacotes do tipo especificado por você.
- **Atual:** O pacote selecionado atualmente.

Uso da página Atribuir códigos de retorno

Use a página **Atribuir códigos de retorno** para configurar mensagens de status do pacote de distribuição que aparecem no console dependendo se uma tarefa de distribuição funcionar ou não.

A página **Atribuir códigos de retorno** contém as seguintes opções:

- **Informações do pacote:** Contém um resumo de propriedades para o pacote de distribuição.
  - **Nome do pacote:** Mostra o nome do pacote de distribuição.
  - **Tipo de pacote:** Mostra o tipo de pacote (MSI, EXE, BAT etc.).
  - **Modelo designado:** Mostra o modelo de código de retorno que foi associado ao pacote de distribuição.
- **Informações de modelo do código de retorno:** Mostra o nome, descrição e data de modificação para todos os modelos disponíveis. Para associar um modelo específico a um pacote de distribuição clique no modelo e clique no botão **Atribuir**.
- **Modificar:** Modifica o modelo e abre a janela Mapeamentos de código de retorno de pacote.
- **Atribuir:** Associa o modelo selecionado atualmente ao pacote de distribuição.

Uso do Gerenciador de modelo de código de retorno

Use o **Gerenciador de modelo de código de retorno** para adicionar, modificar, excluir, importar e exportar modelos de código de retorno. Você pode mostrar esta caixa de diálogo da ferramenta Pacotes de distribuição clicando no botão **Gerenciador de modelo de código de retorno** da barra de ferramenta. A caixa de diálogo **Gerenciador de modelo de código de retorno** contém as seguintes opções:

- **Informações de modelo do código de retorno:** Relaciona todos os modelos existentes por nome, descrição, tipo e data de modificação.
- **Tipo de filtro de modelo:** Filtra a lista de modelos para mostrar Todos, MSI ou Outro.
- **Nome do modelo:** Mostra o nome a ser atribuído ao novo modelo.
- **Descrição do modelo:** Mostra o nome a ser atribuído ao novo modelo.

- **Tipo de filtro de modelo**: Mostra o grupo a ser atribuído ao novo modelo para opções de filtragem. Escolhe entre MSI ou Outro.
- **Adicionar:** Abre a janela Novo modelo de mapeamento de código de retorno.
- **Modificar:** Abra a janela Mapeamentos de código de retorno de pacote para habilitar um usuário a modificar o modelo selecionado.
- **Excluir:** remove o modelo selecionado.
- **Importar:** Permite importar um modelo de um local designado (formato .xml).
- **Exportar:** Permite exportar um modelo de um local designado (formato .xml).

Uso da caixa de diálogo Mapeamentos de código de retorno de pacote

A janela Mapeamento do código de retorno de pacote contém as seguintes opções:

- **Informações de modelo do código de retorno:** Contém as propriedades gerais do modelo.
  - **Nome do modelo:** Mostra o nome do modelo que foi atribuído no Gerenciador de modelo de código de retorno.
  - **Descrição do modelo:** Mostra a descrição do modelo que foi atribuído no Gerenciador de modelo de código de retorno.
- **Comportamento padrão:**
  - **Estado:** Atribui um estado de êxito ou falha.
  - **Mensagem:** Insere uma mensagem personalizada que será mostrada se o pacote enviar o código de retorno selecionado.
- **Mapeamentos de código de retorno:** Atribui novos códigos de retorno ou remove os existentes usando os botões **Adicionar** ou **Excluir** (lado direito). Os códigos de retorno adicionados desta forma serão criados em ordem numérica.
- **Editar mapeamentos de código de retorno:** Insere os números dos códigos de retorno a serem criados. Clique no botão **Aplicar** após fazer adições e modificações nesta seção.
  - **Único:** Permite a atribuição de um número de código de retorno único que pode então ser atribuído a um estado e uma mensagem personalizada.
  - **Faixa:** Permite a atribuição de uma faixa de números de código de retorno que podem então ser atribuída a um estado e uma mensagem personalizada.
- **Mensagem:** Mostra a mensagem personalizada quando o pacote envia o código de retorno.
- **Estado:** Configura o código de retorno para indicar êxito ou falha.

Usando a página de opções do pacote de SWD

Use essa página para definir o que ocorrerá quando um pacote de SWD já estiver instalado em um dispositivo. Se tiver aplicativos que não respondem a um reparo de pacote normal, a opção de reinstalação completa poderá funcionar melhor. O reparo tende a levar menos tempo do que uma reinstalação completa.

Quando se cria um pacote de SWD, é possível criá-lo com ou sem a interface de instalação de pacotes que os usuários vêem. Se o pacote tem uma interface, você pode escolher entre exibir a caixa de diálogo de status da instalação do pacote por cima dos aplicativos existentes, ou se o pano de fundo da instalação que cobre a área de trabalho deve ser exibido em azul sólido enquanto o pacote é instalado.

- **Reparar (corrigir) o pacote:** Essa opção somente atualiza as chaves do registro e substitui os arquivos de programa que o agente detecta como diferentes daqueles existentes no pacote de instalação.

- **Executar uma reinstalação completa do pacote:** Essa opção reinstala completamente o pacote, substituindo todos os arquivos e recriando todas as chaves do registro.
- **Quando os comentários estiverem habilitados, sobregravar as configurações acima e permitir ao usuário decidir:** Permitir aos usuários escolher entre reparar ou reinstalar. Você pode habilitar o feedback na caixa de diálogo **Propriedades de método de distribuição** da página **Feedback**.
- **Quando o comentário estiver habilitado, exibir a tela de fundo:** Mostra uma tela de fundo em azul. Você pode habilitar o feedback na caixa de diálogo **Propriedades de método de distribuição** da página **Feedback**.

Usando a caixa de diálogo Métodos de entrega

A caixa de diálogo **Métodos de entrega** (**Ferramentas > Distribuição > Métodos de entrega**) define como o pacote será enviado para os dispositivos. Estas opções não estão associadas a nenhum pacote de distribuição específico. As opções incluem a Multidifusão dirigida, o envio (Push) e distribuições baseadas em diretivas. Não crie um método de entrega todas as vezes que desejar distribuir um pacote. O ideal é criar um gabarito (ou modelo) de método de entrega para ser reusado para distribuições que utilizam o mesmo método de entrega.

Antes de usar esta caixa de diálogo, crie o pacote de distribuição (**Ferramentas > Distribuição >| Pacote de distribuição**) que você deseja distribuir.

Sobre a página Descrição

Use esta página para descrever o método de entrega que está sendo criado e para determinar o número de dispositivos para os quais você deseja distribuir simultaneamente.

- **Nome:** O nome do seu método de entrega.
- **Proprietário:** o nome da pessoa que criou o pacote originalmente. Você não pode mudar este campo.
- **Descrição do método de entrega:** O nome que for digitado aqui aparece nas árvores e caixas de diálogos dos **Pacotes de distribuição** e **Métodos de entrega**. Use um nome descritivo, mas não muito longo, já que você terá de rolar a tela para poder ver descrições longas.
- **Número de computadores para distribuição:** Controla o número máximo de dispositivos que podem receber simultaneamente a distribuição de software.

Sobre a página de uso da rede

Use esta página para controlar a maneira de como o pacote e os arquivos de pacote são enviados aos dispositivos gerenciados. Você terá estas opções:

- **Usar multidifusão para distribuir arquivos:** Usa a multidifusão dirigida para enviar arquivos simultaneamente a vários dispositivos.
- **Use executar da origem para distribuir arquivos:** não copia arquivos localmente antes de instalá-los. Em vez disso, o arquivo de pacote primário é executado diretamente do local de descarregamento do pacote. Essa opção funciona com todos os tipos de pacotes nos compartilhamentos UNC. Para os compartilhamentos HTTP, essa opção só funciona com os tipos de pacotes SWD e MSI. Use essa opção com instalações de aplicativos que requeiram uma estrutura de pasta específica. Essa opção usará servidores preferenciais mas não rodará o pacote de um parceiro.
- **Use download da origem para distribuir arquivos:** Cada dispositivo descarrega arquivos de pacote do servidor de pacotes antes de usá-los. Essa opção não aproveita da Multidifusão dirigida.

Sobre a página Largura de banda (sob a página Utilização da rede)

Use essa página para controlar a largura de banda da rede que o pacote exige para implantação. Não é necessário selecionar nenhuma dessas opções se você desejar que todos os clientes selecionados recebam o pacote independentemente da largura de banda.

O controle da largura de banda é importante para dispositivos cuja conexão WAN ou dial-up seja lenta. Geralmente, você não desejará distribuir um pacote com muitos megabyte para dispositivos em links lentos. Escolha as seguintes opções:

- **Exigir uma conexão de rede não-RAS:** Essa opção habilita o requisito de largura de banda. Selecione uma das seguintes opções:
    - **Permitir qualquer conexão de rede não-RAS:** Essa opção permite que dispositivos em WANs e LANs recebam o pacote.
    - **Exige uma conexão de rede de alta velocidade:** Essa opção só permite que clientes em uma LAN recebam o pacote.
- **Limitar downloads remotos (por sub-rede) a um dispositivo de cada vez:** Use esta opção para reduzir a largura de banda de rede consumida em uma sub-rede.
    - **Porcentagem máxima de largura de banda a usar:** Após ter escolhido Limitar downloads remotos, você pode limitar ainda mais a largura de banda através do ajuste da porcentagem máxima da largura de banda da rede do dispositivo alvo a ser usada para a distribuição.

Se você estiver usando PDS para detectar a velocidade de conexão da rede, as conexões de alta velocidade e baixa velocidade retornarão as mesmas informações. Para uma detecção precisa das conexões de rede de alta velocidade, você precisa usar o ICMP.

O ICMP envia solicitações de eco de ICMP de vários tamanhos para o computador remoto e usa o tempo de ida e volta dessas solicitações/respostas de eco para determinar a largura de banda aproximada. No entanto, nem todos os roteadores ou computadores oferecem suporte ao encaminhamento ou resposta às solicitações de eco de ICMP. O ICMP também distingue entre conexões LAN (alta velocidade) e WAN (lenta, mas não dial-up).

Se sua rede não estiver configurada para permitir solicitações de eco de ICMP, será possível selecionar o PDS. Se estiver usando o PDS, a opção **Exigir uma conexão de rede de alta velocidade** não fornecerá um controle preciso.

Sobre a página Uso da largura de banda (sob a página Uso da rede)

Use essa página para configurar o limite de largura de banda e os atrasos de transmissão de pacotes.

- **Download de parceiro (só instalar do cache ou parceiro):** Talvez não seja visível em todas as caixas de diálogos de **Uso de largura de banda**. Permite o download de pacotes somente se eles estiverem na cache local ou em um parceiro no mesmo domínio de multidifusão. Essa opção conserva a largura de banda da rede, mas para que a instalação do pacote seja bem-sucedida, o pacote deve estar em um desses dois locais.
- **A largura de banda usada do núcleo ou do servidor preferencial (WAN):** Ajusta a prioridade desta tarefa específica acima de outro tráfego de rede. Quanto mais alta for a porcentagem do deslizador, maior será a quantidade de largura de banda usada por esta tarefa acima de qualquer outro tráfego. As conexões WAN em geral são mais lentas, por isso recomenda-se com frequência colocar este deslizador na porcentagem mais baixa.

- **Largura de banda usada parceiro a parceiro (peer-to-peer) (Local):** Ajusta a prioridade desta tarefa específica acima de outro tráfego de rede. Quanto mais alta for a porcentagem do deslizador, maior será a quantidade de largura de banda usada por esta tarefa acima de qualquer outro tráfego. As conexões de LAN são, em geral, mais rápidas que as conexões WAN, por isso recomendada-se frequentemente que o slider seja definido em uma porcentagem mais alta que a WAN.

Sobre a página Domínio de multidifusão (sob a página Utilização da rede)

Essa página será exibida apenas quando você tiver selecionado Multidifusão como o tipo de distribuição. Use essa página para configurar as opções de multidifusão.

- **Usar o Descobrimento de domínio de multidifusão:** Use essa opção apenas se quiser que a Multidifusão dirigida descubra um domínio para a tarefa em questão. Essa opção não salvará os resultados do descobrimento de domínio para que sejam reutilizados.
- **Usar descobrimento de domínio de multidifusão e salvar resultados:** Use essa opção apenas se quiser que a Multidifusão dirigida descubra um domínio para a tarefa em questão e salve os resultados para uso posterior, economizando tempo em multidifusões subseqüentes.
- **Usar os resultados do último descobrimento de domínio de multidifusão:** Use essa opção quando a Multidifusão dirigida tiver descoberto um domínio e salvo os resultados.
- **Representantes de domínio ativam dispositivos gerenciados:** Use esta opção se desejar que os computadores que ofereçam suporte à tecnologia Wake On LAN sejam ligados para que possam receber a multidifusão. Você pode usar a caixa de diálogo Opções de multidifusão para configurar o tempo que os representantes de domínio devem aguardar para fazer a multidifusão após o envio do pacote Wake On LAN. O período de espera padrão é de 120 segundos.
- **Número de segundos a esperar Wake on LAN:** Tempo de espera dos representantes de domínio para fazer a multidifusão depois que o pacote Wake On LAN for enviado. O período de espera padrão é de 120 segundos. Se alguns computadores na rede demorarem mais do que 120 segundos para a reinicialização, você deverá aumentar esse valor. O valor máximo permitido é 3600 segundos (uma hora).

Sobre a descoberta de domínio

A descoberta de domínio é necessária apenas em redes com sub-redes que possam ver o tráfego de multidifusão entre elas. Se as sub-redes não puderem ver os tráfegos umas das outras, você poderá economizar tempo salvando primeiro os resultados de uma descoberta de domínio e então selecionando **Usar resultados da última descoberta de domínio de multidifusão** de modo que a Multidifusão dirigida não execute uma descoberta de domínio antes de cada trabalho.

Se as sub-redes de sua rede enxergarem o tráfego de multidifusão umas das outras, você poderá ajudar a Multidifusão dirigida a trabalhar mais rápido descobrindo previamente seus domínios com o script multicast_ domain_discovery.ini incluído na pasta ManagementSuite\Scripts. Esse script não faz nada nos dispositivos alvo. Execute esse script na janela **Tarefas agendadas** mediante uma lista de alvos que estende sua rede. Isso salvará os resultados da descoberta de domínio para uso posterior. Talvez você queira executar esse script periodicamente com grandes conjuntos de distribuição de multidifusão.

Se selecionar **Usar arquivo em cache** em **Configurar > Serviços > Multidifusão**, a Multidifusão dirigida passará por um processo de descoberta, mesmo se a opção **Usar os resultados da última descoberta de domínio de multidifusão** for selecionada. A Multidifusão dirigida precisa realizar esse procedimento para descobrir quais representantes de domínio de multidifusão em potencial têm o arquivo em cache.

Sobre a página Limites de multidifusão (sob a página Utilização da rede)

Use esta página para configurar parâmetros de Multidifusão dirigida específicos para a tarefa. Os padrões nessa caixa de diálogo devem funcionar para a maioria das multidifusões.

- **Número máximo de representantes do domínio de multidifusão trabalhando simultaneamente:** Não mais do que este número de representantes executará uma multidifusão simultaneamente. O padrão é 5.
- **Número máximo de dispositivos onde a multidifusão não pôde processar simultaneamente:** Quando um dispositivo apresentar falha ao receber o arquivo através de multidifusão, ele fará o download do arquivo do servidor Web ou de arquivos. Esse parâmetro pode ser usado para limitar o número de dispositivos que obterão o arquivo de uma só vez. Por exemplo, se o número máximo de segmentos (threads) fosse 200 e o número máximo de segmentos com falha de multidifusão fosse 20, o manipulador de Tarefas personalizadas processaria por vez não mais do que 20 computadores que apresentassem falha de multidifusão. O manipulador de Tarefas personalizadas processará no máximo 200 dispositivos por vez se eles receberem com êxito a multidifusão, mas não mais do que 20 desses 200 segmentos processarão os clientes que apresentarem falha na tarefa de multidifusão. Se esse valor for definido como 0, o manipulador de tarefas personalizadas não executará a parte de distribuição da tarefa para nenhum computador que tiver apresentado falha na multidifusão. O padrão é 240.
- **Número de dias que os arquivos permanecem no cache do dispositivo:** Tempo em que o arquivo sendo transmitido por multidifusão pode permanecer no cache de cada computador alvo. Após esse período, o arquivo será automaticamente removido. O padrão é 2.
- **Número de dias que os arquivos permanecem no cache do representante de domínio de multidifusão:** Tempo em que o arquivo sendo transmitido por multidifusão pode permanecer no cache do representante de domínio de multidifusão. Após esse período, o arquivo será automaticamente removido. O padrão é 14.

Sobre a página Reinicializar

Use essa página para configurar se o computador será reinicializado depois que o software for instalado ou removido. Você terá três opções:

- **Reinicializar se for necessário:** Os dispositivos reinicializarão se o pacote assim exigir.
- **Nunca reinicializar:** os clientes não reinicializarão após a instalação de um pacote. Se você selecionar essa configuração e seu pacote exigir uma reinicialização, os clientes poderão encontrar erros ao executar o aplicativo até serem reinicializados. Se o pacote for SWD, essa opção anulará qualquer configuração no pacote. Se o pacote for um executável genérico ou um pacote MSI, sua configuração poderá anular essa opção.
- **Sempre reinicializar:** Os dispositivos reinicializarão independentemente de o pacote exigir ou não.

Sobre a página Feedback e horário

Use essa página para ajudar a determinar o que o usuário verá durante a instalação ou remoção do software. Você terá estas opções:

- **Interface de usuário de andamento de pacote:**
    - **Ocultar todos os comentários do usuário:** Oculta a instalação do usuário tanto quanto o pacote de distribuição de software permitir. Esta opção é dependente de se o pacote de distribuição de software foi ou não criado para ser silencioso.

    - **Mostrar o andamento ao usuário** Habilita a caixa de mensagem de notificação da instalação do software e a animação do ícone da bandeja do sistema durante a instalação do software. Também habilita as seguintes opções:
- **Executar o pacote imediatamente:** Instala o pacote imediatamente sem permitir atrasos.
- **Permite ao usuário atrasar a execução do pacote:** Habilita intervalos para que os usuários possam atrasar as instalações de pacote. Isso pode ajudar os usuários no meio de uma tarefa à qual a instalação do pacote possa interferir.
    - **Pospor automaticamente até o próximo login:** Quando marcado, a instalação do pacote é atrasada até o próximo login sem avisar os usuários. Após o próximo login, os usuários verão a caixa de diálogo de intervalo se você marcar **Usuário seleciona o atraso**.
    - **Avisar o usuário antes de descarregar o pacote:** Notivica o usuário antes de um dispositivo gerenciado iniciar o download do pacote. Esta opção é particularmente útil se for usada com opções de adiamento para impedir que um usuário seja forçado a descarregar um aplicativo grande através de uma conexão lenta.
    - **Avisar o usuário antes de executar o pacote:** Mostra uma mensagem antes de iniciar a instalação após o pacote ser descarregado para o cache local de distribuição.
- **Permitir ao usuário cancelar:** Essa opção permite que o usuário cancele a ação (uma instalação ou remoção). Em geral, para as diretivas de aplicativo, isso não é recomendado.
- **Exibir interface completa do pacote:** Esta opção controla se a instalação do pacote é silenciosa (desativada) ou solicita o feedback do usuário quando necessário (ativada).
- **Mostrar status de sucesso ou falha ao usuário final:** Exibe uma caixa de diálogo após a instalação do pacote mostrando se a instalação foi concluída com sucesso ou não.

Sobre a página Mais opções de intervalos (sob a página feedback e horário)

Esta página é usada para configurar os limites de intervalo do pacote e as opções de limite de tempo. As opções nesta página são habilitadas clicando-se na opção **Usuário seleciona o atraso** da página **Feedback e horário**.

- **Limites de adiamento**
    - **Tempo que o usuário pode pospor o pacote:** Seleciona as horas, os minutos ou os segundos de atraso dos pacotes se o usuário clicar em **Aguardar** na caixa de diálogo de intervalos.
    - **Atraso do usuário é limitado:** Limita o número de vezes que os usuários podem clicar em **Aguardar** quando aparece a caixa de diálogo de intervalos.
    - **Número de vezes que o usuário pode pospor:** O limite do atraso.

- **Comportamento de usuário desconectado**
  - **Continuar instalação:** Este é o padrão. Continua a instalação quando o usuário está desconectados.

    Observe que as configurações da conta de instalação do pacote na página de **Contas** nas propriedades do pacote substituem as opções de comportamento do usuário desconectado em um método de distribuição.

    Se você selecionar instalar como usuário atual nas propriedades do pacote e selecione **Continuar instalação** de usuários desconectados no método de entrega, o conflito causará a falha da instalação do pacote nos dispositivos onde o usuário atual não está conectado.
  - Falha na instalação: Falha na instalação se o usuário estiver desconectado, independentemente das configurações da conta nas propriedades do pacote.
- **Comportamento do usuário conectados e opções de tempo excedido**
  - **Aguardar resposta do usuário antes de continuar:** A caixa de diálogo de intervalos e aguarda a resposta do usuário. Isso acontece independentemente do atraso especificado. A tarefa atingirá o tempo limite e falhará se os usuários demorarem muito para responder ou se não houver ninguém no computador.

    Quando o feedback do usuário for necessário, você poderá escolher a ação padrão em uma lista. Clique no botão radial ao lado da lista e selecione **Cancelar**, **Executar o pacote** ou **Atrasar**. Você pode digitar o tempo no qual a caixa de diálogo de intervalos deve aguardar por uma resposta antes de completar a ação selecionada.
  - **Tempo antes que a ação acima inicie automaticamente:** Tempo antes que a ação na lista suspensa seja completada.

Sobre a página mensagem personalizada (sob a página feedback e horário)

Use esta página se quiser configurar uma mensagem personalizada para a caixa de diálogo de intervalos. Esta caixa de diálogo só aparece se você permitir atrasos. A origem da página HTML para as páginas de atraso está no servidor núcleo da pasta LDLogon\html\.

- **Uso das páginas personalizadas HTML:** Usa as páginas HTML na pasta LDLogon\html\ do servidor núcleo.
- **Incluir uma mensagem personalizada na caixa de diálogo de intervalos:** Acrescenta texto que você digita na caixa de diálogo de intervalos (inclusive formatação HTML), substituindo o texto padrão que é normalmente inserido. A caixa de diálogo ainda pode mostrar os botões **Aguardar**, **Cancelar** e **Instalar agora** com texto descrevendo cada ação.

Sobre o Tipo e freqüência da página de diretiva

Esta página aparece para tipos de entrega baseados em diretivas e afeta o modo como os dispositivos alvo agem quando recebem a diretiva.

- **Obrigatórias:** O agente de entrega baseado em diretivas aplica automaticamente as diretivas necessárias sem a intervenção do usuário. Você pode configurar as diretivas obrigatórias para serem executadas silenciosamente. Qualquer UI que apareça no dispositivo, enquanto uma tarefa obrigatória estiver sendo instalada, não deverá ser bloqueada; em outras palavras, o aplicativo que estiver sendo instalado não deve exigir intervenção do usuário.
- **Recomendadas:** Os usuários têm a opção de determinar quando as diretivas recomendadas devem ser instaladas. As diretivas recomendadas são selecionadas por padrão na UI do cliente.

- **Opcionais:** Os usuários têm a opção de determinar quando as diretivas opcionais devem ser instaladas. As diretivas opcionais não são selecionadas por padrão na UI do cliente.

Você pode também configurar a freqüência com que uma diretiva pode ser executada:

- **Única:** Se uma diretiva for executada com êxito em um dispositivo, o dispositivo não executará essa diretiva novamente.
- **Como desejado:** O pacote pode ser instalado pelos usuários a qualquer momento.
- **Periódica:** Se uma diretiva recomendada ou opcional for especificada como periódica, ela será removida da UI, quando processada com êxito, e será mostrada novamente na UI após o intervalo especificado.

Sobre a página Offline

Use esta página para configurar o que acontece quando um dispositivo está pronto para instalar um pacote mas não pode conectar-se ao servidor núcleo. Isto pode acontecer quando os arquivos de um pacote estão em um cache local de distribuição do dispositivo e um usuário que está viajando, ou que não tem uma conexão de rede, tenta instalar esse pacote.

- **Espere até que o dispositivo possa conectar-se com o servidor núcleo gerenciado:** Só permita a instalação se o dispositivo puder verificar-se a integridade do arquivo de cache de distribuição do pacote com o servidor núcleo. Esta é a opção mais segura.
- **Instalar pacote(s) offline:** Permite que o pacote instale a partir dos arquivos existentes no cache de distribuição sem exigir uma conexão ao servidor núcleo.

Sobre a página Redução (Downgrade)

Use esta página para configurar o comportamento da distribuição quando o sistema operacional do alvo ou os agentes do dispositivo alvo não oferecerem suporte aos métodos de entrega que você tiver escolhido. Por exemplo, se houver agentes mais antigos do Management Suite instalados nos dispositivos, eles poderão não oferecer suporte à multidifusão ou ao download de parceiros.

Opções de redução do SO:

- **Reduzir a funcionalidade ao nível do sistema operacional:** Permite que as tarefas continuem, embora nenhuma das opções selecionadas de método de entrega esteja ativa.
- **Com falha se o sistema operacional não pode lidar com a funcionalidade padrão:** A tarefa falha se o sistema operacional não oferecer suporte às opções selecionadas de método de entrega.

Opções de redução do dispositivo:

- **Reduzir a funcionalidade ao nível do agente:** Permite que a tarefa continue, embora nenhuma das opções selecionadas de método de entrega esteja ativa.
- **Falha se o agente não pode lidar com a funcionalidade padrão:** A tarefa falha se os agentes não oferecerem suporte às opções selecionadas de método de entrega.

Sobre a página Descoberta

Esta página permite que você escolha as opções para a descoberta de dispositivos. Antes do manipulador de tarefas personalizados poder processar uma tarefa, ele precisa descobrir o endereço IP atual de cada dispositivo. Esta guia permite configurar a forma como o serviço contata os dispositivos.

Opções de descoberta:

- **UDP:** A seleção de UDP usa um ping de PDS (Ping Discovery Service) via UDP. A maioria dos componentes de dispositivos do Management Suite dependem do PDS, portanto seus dispositivos gerenciados devem ter o PDS instalado. O PDS é parte do agente LANDesk padrão. Este é o método de descoberta mais rápido e o padrão. Com UDP, você pode também selecionar Novas Tentativas e Tempo limite de ping UDP.
- **TCP:** A seleção de TCP usa uma conexão HTTP para o dispositivo na porta 9595. Esse método de descoberta oferece o benefício de ser capaz de funcionar através de uma firewall se você abrir a porta 9595, mas está sujeito a tempos limites de conexão de HTTP se os dispositivos não estiverem presentes. Esses tempos limite podem durar 20 segundos ou mais. Se um grupo de dispositivos alvo não responder à conexão TCP, a sua tarefa levará algum tempo para começar.
- **Ambos:** A seleção de Ambos faz o serviço tentar a descoberta com UDP primeiro, com TCP e, por último, com DNS/WINS, se selecionado.
- **Número de novas tentativas:** números de tentativas de descoberta a fazer.
- **Tempo limite da descoberta:** tempo da espera para uma resposta em cada tentativa de descoberta.
- **Tempo limite para transmissão de sub-rede:** tempo da espera para uma resposta da difusões de sub-rede.
- **Desabilitar transmissão de sub-rede:** Desabilita a descoberta via difusão de sub-rede. Quando selecionada, esta opção resultará em uma transmissão direcionada a uma sub-rede sendo enviada através de UDP usando PDS.
- **Desabilitar procura de DNS/WINS** Desabilita uma pesquisa de serviço de nomes para cada dispositivo se o método de descoberta TCP/UDP falhar.

Sobre a janela Status de distribuição de software por multidifusão

Essa janela aparece no núcleo quando está ocorrendo uma distribuição ativa por Multidifusão dirigida. Ela mostra as seguintes informações:

- **Endereço URL ou UNC do pacote:** Essa é a localização do pacote que você está tentando distribuir no momento. Esta linha será atualizada com o arquivo atual sendo transferido.
- **Status:** Um relatório em tempo real sobre como está a distribuição ou, se a distribuição tiver sido concluída, a forma como a tarefa foi concluída.
- **Domínios de multidifusão:** O campo na parte superior mostra todas as sub-redes e os representantes de domínio de multidifusão que estão sendo usados na distribuição. Quando você destaca cada representante de domínio, a janela inferior exibe todos os computadores que estão recebendo a distribuição do representante de domínio.
  Cada computador na janela inferior contém informações sobre como a distribuição foi concluída no computador. Existem vários campos de informações à direita de cada computador relacionado, incluindo Pacotes perdidos, Solicitações de reenvio e Solicitações de redução. Esses campos não contem informações até que a distribuição esteja concluída.
- **Pacotes ausentes:** Mostra o número de pacotes que o dispositivo não conseguiu obter do representante da sub-rede. Se esse número não for 0, a distribuição falhou.
- **Solicitações de reenvio:** Mostra o número de vezes que o dispositivo teve que solicitar o reenvio dos pacotes no representante da sub-rede. Essa é uma boa maneira de medir, por exemplo, o nível de ocupação do dispositivo ao lidar com outros processos durante a distribuição.

- **Solicitações de redução:** Mostra o número de vezes que o cliente teve que solicitar ao representante da sub-rede que reduzisse o fluxo de pacotes. Nesse caso, números altos geralmente indicam que um computador está tendo algum problema de hardware que está reduzindo a velocidade da distribuição. Se você tiver um número elevado de computadores que apresentam um número alto de solicitações de redução, será preciso verificar o número de Atraso/Pacotes no representante da sub-rede. Há sempre uma correlação entre o número de Atraso/Pacotes e o número de solicitações de redução.

Essa janela é fechada automaticamente após 10 segundos. Se desejar que a janela permaneça aberta durante toda a distribuição, clique em **Manter diálogo aberto** e a janela ficará aberta até que você a feche manualmente. Manter o diálogo aberto irá parar a execução do script; portanto, feche o diálogo quando terminar.

Criação de scripts personalizados

Use a opção **Criar script personalizado** se quiser criar um script personalizado a partir de um modelo genérico.

Para criar um script personalizado

1. Clique em **Ferramentas > Distribuição > Gerenciar scripts**.
2. No menu de atalho **Todos os outros scripts** , clique em **Criar script personalizado**.
3. Personalizar o script. Se você quiser abrir o script no Notepad ou no editor associado com tipos de arquivos .ini, clique em **Usar editor**. Certifique-se de salvar o arquivo antes de fechar o editor usado para editar o script.
4. Digite um **Nome de script personalizado**. Clique em **OK**.

Criação de scripts de distribuição de arquivos

Se você desejar somente copiar arquivos para os dispositivos, poderá usar um script de distribuição de arquivos. Você pode transferir qualquer tipo de arquivo, incluindo arquivos de texto, para um diretório por você especificado no dispositivo. Os scripts de distribuição de arquivos fornecem suporte à Multidifusão dirigida.

Para distribuir arquivos:

1. Clique em **Ferramentas > Distribuição > Gerenciar scripts**.
2. Clique no botão da barra de ferramentas **Novo script de transferência de arquivos**.
3. Digite um **Nome de script** e o **Diretório de destino**. Clique em **Avançar**.
4. Nas próximas três páginas, selecione a largura da banda, tarefa e opções de multidifusão desejadas.
5. Selecione os arquivos a serem implantados, selecionando um **Caminho da Web** ou um **Caminho de compartilhamento de arquivos**, digitando o caminho e adicionando os arquivos desejados na caixa de listagem. Clique em **Avançar**.
6. Leia o resumo da página **Concluído** e clique em **Concluir**.

As seções a seguir descrevem as páginas e opções do assistente **Criar script de distribuição de arquivo**.

Sobre a página de Informações gerais

Use esta página para configurar as informações gerais do script de transferência de arquivos.

- **Nome do script:** O nome do arquivo para o script. A extensão o nome do arquivo será .ini por padrão. Os scripts são gravados em \Program Files (x86)\LANDesk\ManagementSuite\scripts.
- **Descrição:** A descrição do script que aparece na ferramenta de Gerenciamento de scripts.
- **Diretório de destino:** O diretório nos clientes onde os arquivos distribuídas ficarão guardados.

- **Use multidifusão para distribuir arquivos:** Selecione isso se você quiser usar a multidifusão. Selecionar esta opção habilita os domínios de Multidifusão e as páginas de configuração de Limites de multidifusão.

Sobre a página de opções de Download

Use essa página para configurar o limite de largura de banda e os atrasos de transmissão de pacotes.

- **Download de parceiro (só instalar do cache ou parceiro):** Permite o download de pacotes somente se eles estiverem na cache local ou em um parceiro no mesmo domínio de multidifusão. Essa opção conserva a largura de banda da rede, mas para que a instalação do pacote seja bem-sucedida, o pacote deve estar em um desses dois locais. Uma maneira de usar essa opção é primeiro copiar o pacote para um dispositivo em cada sub-rede com a opção **Armazenar na cache somente os arquivos no computador que usar multidifusão**, anteriormente no assistente.
- **Limite dinâmico da largura de banda:** Especifica que o tráfego de rede que um dispositivo cria tem prioridade sobre o tráfego da distribuição. Se você selecionar essa opção e deixar a **Porcentagem mínima disponível de largura de banda** com o valor 0, quando o dispositivo iniciar o tráfego da rede, a distribuição retornará cerca de um pacote por segundo até o tráfego parar. Essa opção força um download completo do arquivo para a cache do dispositivo, e também permite o reinício do ponto de verificação ao nível de byte, com o qual os downloads são retomados de onde pararem, se forem interrompidos. Se estiver instalando ou reparando um pacote ESWD ou um pacote MSI, você talvez não queira usar a opção **Limite dinâmico da largura de banda**, porque esses tipos de pacote normalmente fazem o download somente dos arquivos de que precisam.
- **Porcentagem mínima disponível de largura de banda a ser usada no cliente:** Especifica a quantidade de Limite dinâmico da largura de banda que deve ser aplicada. Digite valores de até 50 por cento da largura de banda total da rede disponível para o dispositivo. Por exemplo, se um outro aplicativo estivesse consumindo largura de banda de rede no dispositivo durante uma distribuição e você definisse a porcentagem de largura de banda em 50 por cento, a tarefa de distribuição consumiria 50 por cento e o aplicativo do dispositivo consumiria 50 por cento. Na prática, essa porcentagem é variável porque o sistema operacional reserva automaticamente grande parte da largura de banda da rede dependendo do número de aplicativos que necessitam de largura de banda e de sua prioridade.
- **Atraso entre pacotes (parceiro):** essa opção especifica o atraso de transmissão entre pacotes para parceiros na mesma sub-rede. Você pode usar esse atraso para forçar a velocidade das distribuições, tornando-as mais rápidas ou mais lentas. Aumentar o atraso entre pacotes torna a distribuição mais lenta e utiliza menos largura de banda. Você pode usar essa opção com **Limite dinâmico da largura de banda**, mas se essas opções forem usadas em conjunto, o atraso entre pacotes terá mais efeito.
- **Atraso entre pacotes (origem):** Especifica o atraso entre a origem do pacote e o destino do dispositivo. Aumentar o atraso entre pacotes torna a distribuição mais lenta e utiliza menos largura de banda. Você pode usar essa opção com **Limite dinâmico da largura de banda**, mas se essas opções forem usadas em conjunto, o atraso entre pacotes terá mais efeito.

Sobre a página Opções de tarefa

Use essa página para configurar como a distribuição será implantada. Se estiver distribuindo um arquivo MSI ou executável genérico, você terá a opção de inserir qualquer opção de linha de comando que precisar ser transmitida ao arquivo após a multidifusão.

- **O script usa o limite de distribuição padrão:** Você pode limitar o número de computadores aos quais será distribuída a Multidifusão dirigida simultaneamente. Essa opção usa o valor padrão que você definiu em **Configurar > Serviços > Tarefas personalizadas** na opção **Distribuir para X computadores simultaneamente**.

- **O script usa o limite de distribuição personalizado:** Use essa opção para substituir o padrão da tarefa atual especificando um valor diferente.
- **Instalar apenas a partir do cache ou ponto:** Essa opção impede que os computadores alvo vão além de suas sub-redes para instalar um pacote. Os computadores procurarão primeiro em seus diretórios cache de multidifusão; se o pacote não for encontrado, eles verificarão os pontos nas respectivas sub-redes. Se nenhum ponto tiver o pacote, a distribuição falhará. Essa opção minimiza o tráfego da rede em todas as sub-redes. Você poderá usar essa opção quando tiver copiado um pacote para cada sub-rede com a opção **Armazenar na cache somente os arquivos no computador que usar multidifusão** da página Criar scripts.
- **Verifique o arquivo antes de instalar o cliente:** Gera um hash (CRC) para o pacote que você está distribuindo assim que o assistente for finalizado. Os dispositivos podem então usar esse valor de hash para se certificarem de que o pacote/arquivo que receberam não está corrompido. Dependendo do tamanho do pacote/arquivo que você está distribuindo, pode ser necessário aguardar alguns minutos para concluir o cálculo de hash.
- **Não tentar completar tarefas:** use essa opção para não usar o recurso de completar tarefas para tentar novamente as tarefas que falharam. Normalmente, haverá uma nova tentativa das tarefas falhas quando a conclusão de tarefas é instalada nos dispositivos, na próxima vez em que a conclusão de tarefas rodar. Se ainda usar essa opção, as tarefas falhas serão registradas.

Sobre a página Opções de domínio de multidifusão

Essa página será exibida apenas quando você tiver selecionado multidifusão como o tipo de distribuição. Use essa página para configurar as opções de multidifusão.

- **Usar o Descobrimento de domínio de multidifusão:** Use essa opção apenas se quiser que a Multidifusão dirigida descubra um domínio para a tarefa em questão. Essa opção não salvará os resultados do descobrimento de domínio para que sejam reutilizados.
- **Usar descobrimento de domínio de multidifusão e salvar resultados:** Use essa opção apenas se quiser que a Multidifusão dirigida descubra um domínio para a tarefa em questão e salve os resultados para uso posterior, economizando tempo em multidifusões subseqüentes.
- **Usar os resultados do último descobrimento de domínio de multidifusão:** Use essa opção quando a Multidifusão dirigida tiver descoberto um domínio e salvo os resultados.
- **Os representantes de domínio ativam os computadores:** Use esta opção se desejar que os computadores que ofereçam suporte à tecnologia Wake On LAN sejam ligados para que possam receber a multidifusão. Você pode usar a caixa de diálogo **Opções de multidifusão** para configurar o tempo que os representantes de domínio devem aguardar para fazer a multidifusão após o envio do pacote Wake On LAN. O período de espera padrão é de 120 segundos.
- **Opções avançadas de multidifusão:** Use essa opção para definir as opções avançadas. Os padrões são adequados para a maioria das tarefas.

Sobre a descoberta de domínio

A descoberta de domínio é necessária apenas em redes com sub-redes que possam ver o tráfego de multidifusão entre elas. Se as sub-redes não puderem ver os tráfegos umas das outras, você poderá economizar tempo salvando primeiro os resultados de uma descoberta de domínio e então selecionando **Usar resultados da última descoberta de domínio de multidifusão** de modo que a Multidifusão dirigida não execute uma descoberta de domínio antes de cada trabalho.

Se as sub-redes de sua rede enxergarem o tráfego de multidifusão umas das outras, você poderá ajudar a Multidifusão dirigida a trabalhar mais rápido descobrindo previamente seus domínios com o script multicast_domain_discovery.ini incluído na pasta ManagementSuite\scripts. Esse script não faz nada nos computadores alvo. Execute esse script na janela **Tarefas agendadas** mediante uma lista de alvos que estende sua rede. Isso salvará os resultados da descoberta de domínio para uso posterior. Talvez você queira executar esse script periodicamente com grandes conjuntos de distribuição de multidifusão.

Se selecionar **Usar arquivo em cache** em **Configurar > Serviços Management Suite > Multidifusão**, a Multidifusão dirigida passará por um processo de descoberta, mesmo se a opção **Usar os resultados da última descoberta de domínio de multidifusão** for selecionada. A Multidifusão dirigida precisa realizar esse procedimento para descobrir quais representantes de domínio de multidifusão em potencial têm o arquivo em cache.

Sobre a caixa de diálogo Opções de multidifusão

O assistente de distribuição de script de arquivos contém um diálogo **Opções de multidifusão** na qual você pode configurar parâmetros específicos de Multidifusão dirigida a uma tarefa. Os padrões nessa caixa de diálogo devem funcionar para a maioria das multidifusões.

- **Número máximo de representantes do domínio de multidifusão trabalhando simultaneamente:** Não mais do que este número de representantes executará uma multidifusão simultaneamente.
- **Limitar o processamento de computadores cuja multidifusão apresentou falha...:** Quando um dispositivo apresentar falha ao receber o arquivo através de multidifusão, ele fará o download do arquivo do servidor Web ou de arquivos. Esse parâmetro pode ser usado para limitar o número de dispositivos que obterão o arquivo de uma só vez. Por exemplo, se o número máximo de segmentos fosse 200 e o número máximo de segmentos de falha de multi fosse 20, a caixa de diálogo **Tarefa personalizada** processaria por vez não mais do que 20 computadores que apresentassem falha de multidifusão. A caixa de diálogo **Tarefa personalizada** processará no máximo 200 dispositivos por vez se eles receberem com êxito a multi, mas não mais do que 20 desses 200 segmentos processarão os dispositivos que apresentarem falha na tarefa de multi. Se esse valor for definido como 0, a caixa de diálogo **Tarefa personalizada** não executará a parte de distribuição da tarefa para nenhum computador que tiver apresentado falha na multi.
- **Número de dias que os arquivos ficam no cache do cliente:** Tempo em que o arquivo sendo transmitido por multidifusão pode permanecer no cache de cada computador alvo. Após esse período, o arquivo será automaticamente removido.
- **Número de dias que os arquivos ficam no cache do representante de domínio de multidifusão:** Tempo em que o arquivo sendo transmitido por multidifusão pode permanecer no cache do representante de domínio de multidifusão. Após esse período, o arquivo será automaticamente removido.
- **Número mínimo de milissegundos entre as transmissões de pacotes (WAN ou Local):** Tempo mínimo de espera entre envios de pacotes de multidifusão. Esse valor somente será usado quando o representante não estiver fazendo a multidifusão de um arquivo de seu próprio cache. Se esse parâmetro não for especificado, o tempo de inatividade mínimo padrão armazenado no computador do representante da sub-rede/domínio será usado. É possível usar esse parâmetro para limitar o uso de largura de banda na WAN.
- **Número máximo de milissegundos entre as transmissões do pacote (WAN ou Local):** Tempo máximo de espera entre envios de pacotes de multidifusão. Para obter mais informações, consulte Número mínimo de milissegundos entre as transmissões do pacote acima.

- **Número de segundos a aguardar após Wake On LAN:** Tempo de espera dos representantes de domínio para fazer a multidifusão depois que o pacote Wake On LAN for enviado. O período de espera padrão é de 120 segundos. Se alguns computadores na rede demorarem mais do que 120 segundos para a reinicialização, você deverá aumentar esse valor. O valor máximo permitido é 3600 segundos (uma hora).

Sobre a página Selecionar arquivos para distribuição

A página **Selecionar arquivos para distribuição** é exibida no assistente de script de transferência de arquivos.

- **Caminho da Web:** Clique para pacotes armazenados em um servidor Web. Você deve incluir http:// no URL.
- **Caminho do compartilhamento de arquivo:** Clique para pacotes armazenados em um compartilhamento de sessão nula em um servidor de arquivos. Esse caminho deve seguir a convenção de caminho UNC, \\nome_do_servidor\nome_de_compartilhamento\.
- **Procurar:** Clique em **Procurar** para procurar o caminho. Se você tiver clicado em **Caminho da Web**, uma pequena janela do navegador será aberta. Se você clicou em **Caminho do compartilhamento de arquivo**, uma caixa de diálogo Procurar padrão será aberta. Se você desejar procurar um diretório do servidor Web na janela do browser Selecionar local do pacote, deve incluir uma barra final no URL (/), caso contrário a janela do browser exibirá um erro.
- **Adicionar:** Clique em **Adicionar** para adicionar um programa diretamente da caixa de edição de caminho, depois de inserir o caminho completo e o nome do arquivo.
- **Remover:** Selecione um arquivo que adicionou e clique em **Remover** para remover um arquivo da lista.

Sobre a página Concluído

Essa página resume as ações por você selecionadas para implantação do pacote. Antes de continuar, verifique se os dispositivos gerenciados atenderam a todas as exigências relacionadas na seção de advertência.

Se clicar em **Definir como padrão**, as opções de configuração selecionadas por você serão definidas como os valores padrão para esse assistente.

Clique em **Concluir** e poderá agendar o script para distribuição.

Application policy management (APM)

Sobre o gerenciamento baseado em diretivas

O Gerenciamento baseado em diretivas ajuda a gerenciar com facilidade conjuntos de aplicativos em grupos de dispositivos. Com qualquer outra tarefa agendada, as diretivas exigem:

- Um pacote SWD, MSI, executável, arquivo em lote ou pacote Macintosh que criar.
- Um método de distribuição que suporte diretivas, tanto diretivas como instalação por envio suportada por diretiva.
- Alvos das diretivas dos pacotes de distribuição, como os resultados de uma consulta no LDAP ou no banco de dados núcleo.
- Um horário agendado no qual a diretiva deve ser disponibilizada.

O gerenciamento baseado em diretivas periodicamente executa novamente as consultas que você tiver configurado como parte da diretiva, aplicando suas diretivas aos novos dispositivos gerenciados. Por exemplo, talvez você tenha um contêiner Departamento em seu diretório LDAP que contém objetos Usuário. Qualquer usuário cujo objeto Departamento seja "Marketing" usa um conjunto padrão de aplicativos. Após a configuração de uma diretiva para usuários em Marketing, os novos usuários adicionados a Marketing têm automaticamente o conjunto correto de aplicativos instalados em seus computadores.

Use o console para configurar diretivas de aplicativo armazenadas no banco de dados núcleo.

O gerenciamento baseado em diretivas pode distribuir os seguinte tipos de arquivos:

- MSI
- Executável
- Arquivo em lote
- Macintosh
- RPM Linux
- LANDesk Application Virtualization
- Pacote do Windows Script Host (.wsf)
- Pacote SWD herdado:

O fluxo de tarefas do gerenciamento baseado em diretivas é o seguinte:

1. Certifique-se de que os agentes de distribuição de software estejam instalados nos dispositivos.
2. Se não tiver um pacote para o aplicativo para o qual deseja uma diretiva, crie um. Para obter mais informações, consulte "Distribuição de softwares/Distribuição de pacotes/Métodos de entrega" na página 258.
3. Use a janela de pacotes de distribuição para criar uma definição para o pacote.
4. Crie ou selecione um método de entrega baseado em diretiva.
5. Crie uma tarefa de distribuição de software na janela **Tarefas agendadas** e selecione o pacote e o método de entrega acima.
6. Selecione os alvos para as diretivas, que pode incluir qualquer combinação de dispositivos individuais, consultas de banco de dados, grupos de dispositivo, itens e consultas LDAP.

7. Agende a tarefa para execução. Quando ela for executada, a distribuição será disponibilizada por recepção.
8. O serviço de gerenciamento baseado em diretivas no servidor núcleo atualiza periodicamente a lista de alvos das diretivas através da reavaliação dos resultados das consultas no LDAP/banco de dados. Isso ajuda a garantir que o banco de dados núcleo tenha um conjunto atualizado de usuários/computadores alvo.
9. Um usuário faz logon em um dispositivo, estabelece conexão com a rede ou, de alguma outra maneira, inicia o agente do gerenciamento baseado em diretivas.
10. O serviço Gerenciamento baseado em diretivas do servidor núcleo determina as diretivas aplicáveis com base no ID do dispositivo e no usuário conectado, ou no local do dispositivo LDAP.
11. O serviço Gerenciamento baseado em diretivas envia as informações da diretiva de volta para o agente do Gerenciamento baseado em diretivas.
12. Dependendo de como você configurou o dispositivo para tratar as diretivas, o usuário seleciona as diretivas a serem executadas ou as diretivas são automaticamente executadas. Apenas as diretivas recomendadas ou opcionais estão disponíveis na lista do dispositivo. Quando uma diretiva não processada e recomendada estiver na lista, ela será selecionada como padrão. As diretivas periódicas aparecem na lista imediatamente após seu respectivo intervalo de execução. As diretivas selecionadas são executadas em seqüência.
13. O agente do Gerenciamento baseado em diretivas envia os resultados da diretiva ao servidor núcleo, que os armazena no banco de dados núcleo. O recurso de geração de relatórios de status é reportado ao servidor núcleo usando HTTP para obter melhor confiabilidade. Esse status é exibido na janela Tarefas agendadas.

Configuração de diretivas

O gerenciamento baseado em diretivas requer um tipo de pacote de distribuição suportado para qualquer diretiva que você for criar. Você pode criar os pacotes com antecedência ou enquanto estiver criando a diretiva. É aconselhável criar os pacotes anteriormente para testá-los e garantir que estejam funcionando, antes de usá-los em uma diretiva.

Distribuições e diretivas normais podem usar podem usar o mesmo pacote de distribuição. A diferença está na distribuição e não na criação do pacote. Há dois métodos de entrega que suportam distribuição com base em diretiva:

- **Métodos de entrega de diretivas:** O modelo de distribuição somente diretiva. Somente os dispositivos que satisfaçam aos critérios da diretiva recebem o pacote.
- **Métodos de entrega por envio suportado por diretiva:** Modelo combinado de distribuição por envio e diretiva. Primeiro, a distribuição de software tenta instalar o pacote em todos os dispositivos na lista de alvos. Deste modo, você pode fazer uma distribuição inicial usando a Multidifusão dirigida. Em segundo lugar, quaisquer dispositivos que não tiverem recebido o pacote, ou que tiverem sido incluídos na lista de alvos posteriormente (no caso de uma lista de alvos dinâmica), recebem o pacote quando o agente do gerenciamento baseado em diretivas no dispositivo o solicitar.

A principal diferença entre os métodos de entrega padrão e o método de entrega baseado em diretivas é que a caixa de diálogo **Métodos de entrega** do método baseado em diretivas tem uma página de **Tipo e freqüência da tarefa**.

O tipo e a freqüência da tarefa afetam o modo como os dispositivos-alvo atuarão quando receberem a diretiva:

- **Obrigatórias:** O agente do gerenciamento baseado em diretivas aplica automaticamente as diretivas necessárias sem a intervenção do usuário. Você pode configurar as diretivas obrigatórias para serem executadas silenciosamente. Qualquer UI que apareça no dispositivo, enquanto uma tarefa obrigatória estiver sendo instalada, não deverá ser bloqueada; em outras palavras, o aplicativo que estiver sendo instalado não deve exigir intervenção do usuário.
- **Recomendadas:** Os usuários têm a opção de determinar quando as diretivas recomendadas devem ser instaladas. As diretivas recomendadas são selecionadas por padrão na UI do cliente.
- **Opcionais:** Os usuários têm a opção de determinar quando as diretivas opcionais devem ser instaladas. As diretivas opcionais não são selecionadas por padrão na UI do cliente.

Você pode também configurar a freqüência com que uma diretiva pode ser executada:

- **Executar uma vez:** Se uma diretiva for executada com êxito em um dispositivo, o dispositivo não executará essa diretiva novamente.
- **Periódica:** Se uma diretiva recomendada ou opcional for especificada como periódica, ela será removida da UI, quando processada com êxito, e será mostrada novamente na UI após o intervalo especificado.
- **Como desejado:** Podem ser instaladas pelos usuários a qualquer momento.

Criar uma distribuição baseada em diretivas

As distribuições baseadas em diretivas têm efeito logo que a tarefa de diretiva é iniciada e houver alvos resolvidos. As distribuições por envio suportadas por diretiva entram em efeito após a distribuição inicial ser completada.

Para criar uma distribuição baseada em diretivas

1. No console, clique em **Ferramentas > Distribuição > Métodos de entrega**.
2. Com o botão direito do mouse clique ou em **Distribuição baseada em diretivas** ou em **Distribuição por envio baseada em diretiva** e depois em **Novo método de entrega**.
3. Configure as opções do método de entrega desejado. Clique em **Ajuda** para ver mais informações sobre cada página.
4. Configure as opções desejadas do **Tipo e freqüência da diretiva**.
5. Clique em **OK** quando tiver concluído.
6. Clique em **Ferramentas > Distribuição > Tarefas agendadas**.
7. Clique no botão **Criar tarefa de distribuição de software** na barra de ferramentas.
8. Configure as opções da tarefa que desejar e clique em **OK**.
9. Com a tarefa de distribuição baseada em diretivas selecionada, arraste os alvos da diretiva para o painel da janela à direita.

Adicionar alvos de diretivas

Ao criar uma tarefa baseada em diretiva, é sempre uma boa idéia distribuir inicialmente a diretiva para um conjunto alvo pequeno. Nesse caso se ocorrerem problemas durante a distribuição da diretiva, eles só afetarão um conjunto pequeno de usuários. Quando os resultados da distribuição para o pequeno conjunto de usuários tiverem sido validados, adicione outros alvos à diretiva. Quando forem adicionados novos alvos a uma tarefa de diretiva ativa, a diretiva torna-se imediatamente disponível para os dispositivos recém-selecionados ou para os itens LDAP.

Adição de alvos estáticos

O gerenciamento baseado em diretivas pode usar alvos estáticos como alvos da diretiva. Os alvos estáticos correspondem a uma lista de dispositivos ou usuários específicos que não são alterados a menos que você o faça manualmente. Adicione alvos estáticos selecionando dispositivos individuais na tela da rede como alvos. Dispositivos LDAP individuais não podem ser adicionados como alvos estáticos.

Adição de alvos dinâmicos

O gerenciamento baseado em diretivas pode usar consultas para determinar os alvos da diretiva. As consultas são armazenadas somente no banco de dados do núcleo. Para obter mais informações sobre consultas, leia ""Gerenciador de diretórios/consultas" na página 183".

Os alvos dinâmicos podem incluir grupos de dispositivos de tela de rede, objetos LDAP, consultas LDAP e consultas de inventário.

Para que os dispositivos recebam diretivas direcionadas pelo Active Directory, eles precisam ser configurados para fazer o logon no diretório. Isso significa que eles precisam que todo o software de agente esteja instalado corretamente e que iniciem a sessão no diretório correto para que seu nome, totalmente distinto, coincida com o nome direcionado por meio do Gerenciador de diretórios e do Gerenciador de diretivas de aplicativo de tarefas agendadas.

Para selecionar um dispositivo como alvo do LDAP, cada dispositivo Windows deve ter uma conta de computador no controlador de domínio do Active Directory. Isso significa que o computador que estiver sendo usado como dispositivo deve ter feito logon no domínio em que o Active Directory residir. Você não pode simplesmente mapear uma unidade de rede usando o nome de domínio do Windows completamente qualificado. A diretiva não terá efeito dessa maneira.

Para usar o Gerenciador de diretórios para criar uma consulta:

1. Clique em **Ferramentas > Distribuição > Gerenciador de diretórios**.
2. Clique no botão da barra de ferramentas **Gerenciar diretório**.
3. Digite o URL do diretório e as informações de autenticação e clique em **OK**.
4. Clique no ícone da barra de ferramentas **Nova consulta**.
5. Crie a sua consulta. Para obter mais informações, consulte "Consultas LDAP" na página 184.

Entendendo como os escopos afetam a visibilidade das diretivas alvo

Vários escopos podem filtrar o painel de detalhes do gerenciamento baseado em diretivas para uma lista de alvos. Entretanto, o escopo final usado por uma diretiva é sempre o escopo do proprietário de uma tarefa.

Se a tarefa de diretiva fizer parte das **Tarefas comuns** e outro Management Suite usuário com um escopo diferente procurar no painel de detalhes da tarefa (vamos chamar esse segundo usuário de "editor" da lista de alvos), o painel de detalhes de alvos será filtrado pelo escopo do editor. Nesse caso, o editor pode não ver, no painel de detalhes de alvos, todos os alvos nos quais a diretiva será aplicada, pois o escopo do editor pode não permitir que eles vejam todos os alvos no escopo do criador.

Portal de distribuição de software

As diretivas de aplicativo são sempre processadas usando um modelo de instalação por recepção. Os dispositivos consultam o servidor núcleo sobre quais novas diretivas podem ser aplicadas a eles. Quando essa verificação ocorrer, uma caixa de diálogo será exibida no dispositivo mostrando apenas as diretivas não processadas, recomendadas e opcionais, não as diretivas necessárias. Quando uma diretiva não processada e recomendada aparecer na UI, ela será selecionada por padrão para estimular o usuário final a processá-la.

Depois de processada, a diretiva ainda poderá ser exibida na UI se estiver configurada para execução periódica. Nesse caso, ela continuará a ser selecionada, mesmo se for uma diretiva recomendada. Uma diretiva também pode continuar aparecendo na UI se não for aplicada corretamente.

O agente de distribuição de software nos dispositivos gerenciados também fornecem um portal de distribuição de software. O portal procura diretivas que se aplicam ao dispositivo/usuário local, no cache de distribuição de software local. O portal mostra uma página com a lista das diretivas disponíveis. Os usuários podem selecionar uma diretiva na lista e clicar em **Distribuir** para instalar os pacotes associados à diretiva.

Usar o portal de distribuição de softwares

1. Em um dispositivo gerenciado, clique em **Iniciar > Programas > Gerenciamento LANDesk > Gerenciador de desktop**, e clique no botão **Distribuição de softwares**.
2. Selecione as diretivas que deseja aplicar.
3. Clique em **Distribuir**.

NOTA: Você pode atualizar manualmente a lista de diretivas disponíveis clicando no botão **Atualizar** na **Distribuição de softwares**.

Monitoramento de licenças de software

Visão geral da monitoração de licenças de software

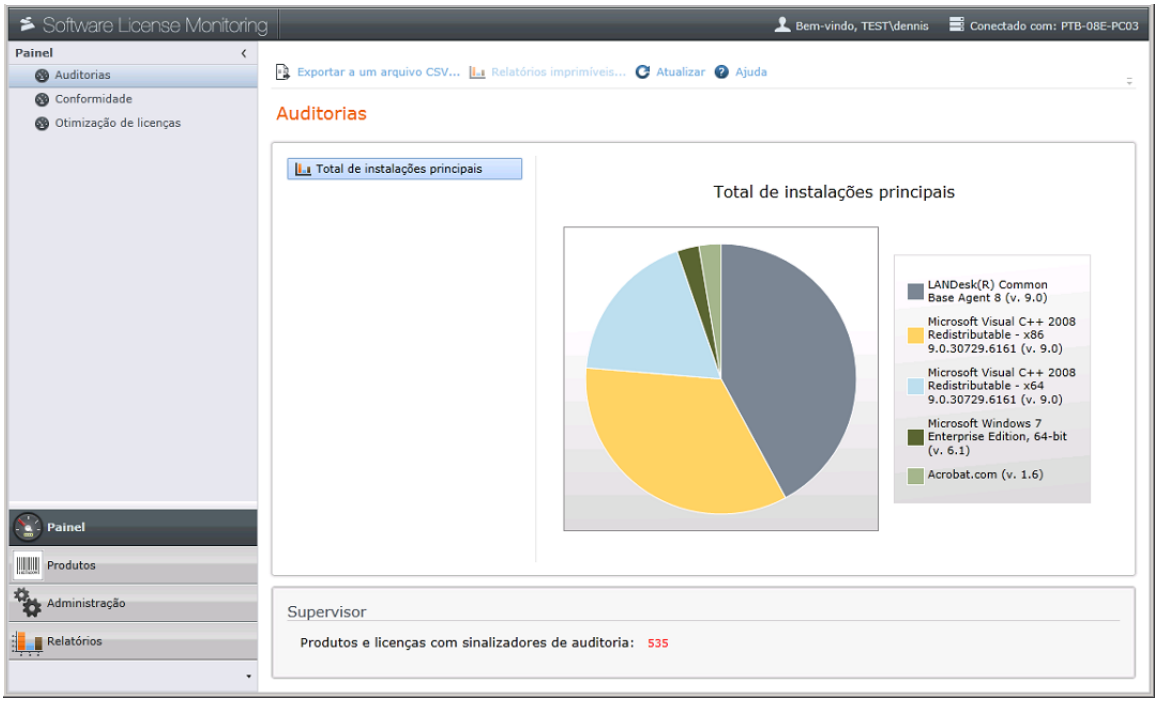
O Monitoramento de licenças de softwares (do inglês, Software license monitoring ou SLM) fornece ferramentas de gerenciamento de ativos de software para que você possa rastrear o uso de softwares, monitorar a conformidade das licenças e controlar os custos de controle de sua empresa.

Os administradores de TI e gerentes de recurso de software acham difícil controlar licenças de produtos instaladas em vários dispositivos em uma rede. Eles correm o risco não apenas de instalar mais produtos do que compraram licenças para, mas também de comprar licenças demais. Você pode evitar estes problemas usando o console do SLM para controlar e informar em licenças de produto e uso através de sua empresa.

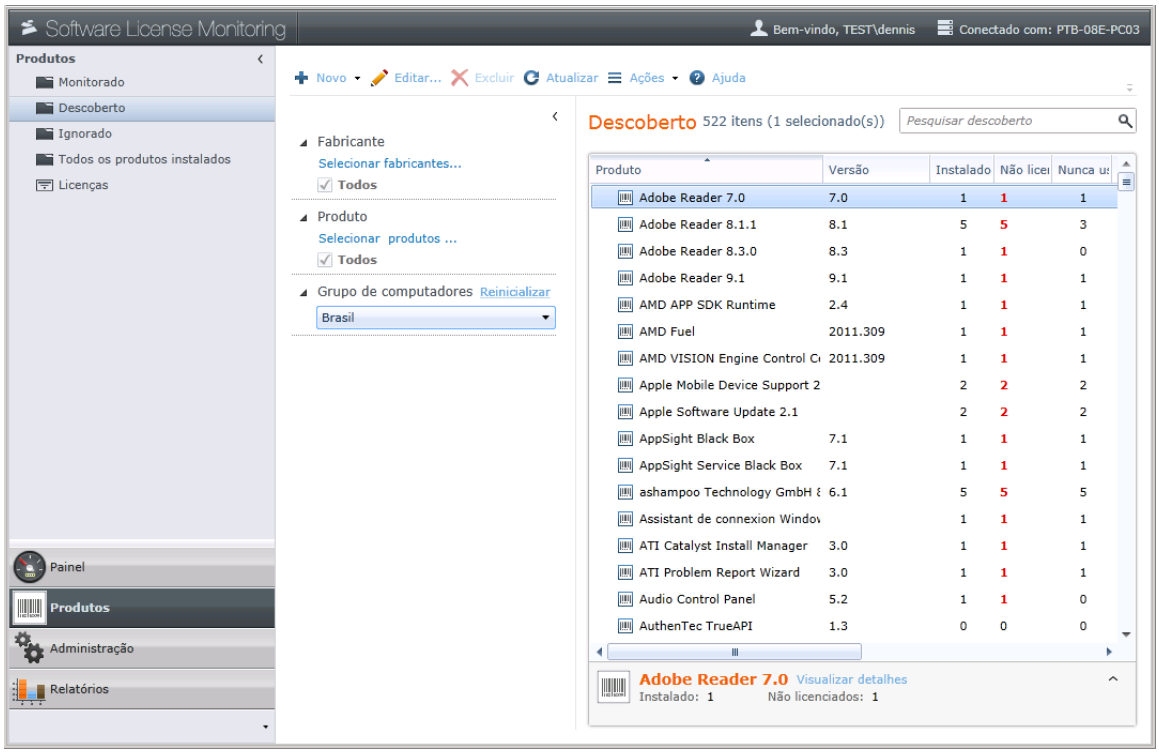
Console do SLM

O console de monitoração de licença de software é iniciado em um navegador da Web. Existem dois tipos de páginas para exibição de dados:

As páginas do **Dashboard** exibem gráficos de resumo do produto chave e dados da licença. São úteis no planejamento da auditoria e para otimizar seu uso de licenças.



As páginas **Produtos** exibem dados detalhados para produtos que são instalados em dispositivos gerenciados. Estas páginas incluem dados de licença usados para calcular conformidade de licença em sua empresa.



Como você trabalha no console do SLM, você gastará a maior parte do tempo no modo de exibição de produto **Monitorado**. Este modo de exibição exibe os produtos que você quer ativamente controlar. Quando você moveu produtos importantes nesta modo de exibição, o modo de exibição **Descoberto** é onde você procurará novo produtos que talvez necessitem sua atenção. Os produtos que você não deve controlar pode ser movido do modo de exibição **Ignorado** para que saiam do caminho.

Se você não está seguro onde um produto é, abra os **Todos os produtos instalados** e procure-o. Você então pode mover o produto ao modo de exibição apropriada (Monitorado ou Ignorado).

Abertura do console

Usuários com uma definição de função que inclua o monitoramento de licença podem ver e editar dados no console de monitoramento de licenças de software. Os usuários administrativos recebem a atribuição desta função como padrão. Outros usuário podem receber permissões de Visualizar e Editar a função de monitoração de licença de software.

Para obter informações sobre mudar permissões de usuário, veja "Funções de gerenciamento" na página 43

IMPORTANTE: O navegador que você usa para exibir o console do SLM deve desativar o bloqueio de pop-ups. Se ativado, é possível que você não consiga ver caixas de diálogos que são abertas a partir do console do SLM. Se você tem problemas exibindo itens no console do SLM, certifique-se que o bloqueador de pop-up está desativado.

Recursos

Os recursos de monitoramento de licenças de software incluem:

- Relatório facilmente acessível sobre conformidade de licença e uso de aplicativo.
- Compartilhamento de licenças de produto. Para alguns produtos, uma nova versão de um produto pode emprestar uma licença de versões anteriores, mantendo seus dispositivos em conformidade o tempo todo.
- A configuração fácil dos parâmetros de licença, incluindo informações sobre aquisições, o tipo de licença, a quantidade e o número de série.
- Os recursos de relatório abrangente de dados, incluindo o número de vezes que cada aplicativo licenciado foi iniciado, a data da última utilização e a duração total da utilização do aplicativo.
- A reconciliação e o controle da instalação, incluindo itens que você controla como licença e a localização física do dispositivo no qual a licença está instalada, bem como notas adicionais.
- Inventário de dispositivos móveis. Os agente monitora o uso de dispositivos portáteis que estão desconectados da rede e envia os dados para o servidor núcleo quando o dispositivo estiver conectado à rede.
- Monitoramento de largura de banda baixa, passiva. O agente de monitoração de software monitora passivamente o uso do produto em dispositivos, usando o mínimo de largura de banda.
- Descoberta automática de produto procurar aplicativos instalados em dispositivos gerenciados, reunindo dados baseados nos arquivos que são associados com esses aplicativos.

Tarefas de monitoramento de licenças de software

Como você controla instalação de produto e uso de licença, você fará as seguintes tarefas gerais.

Obter dados precisos de softwares

O agente de monitoramento de software do Management Suite obtém dados de inventário dos dispositivos gerenciados, como quais aplicativos estão instalados e com que frequência são executados. Esses dados são entregues ao servidor núcleo toda vez que uma análise de inventário de software é concluída. Ao revisar estes dados você pode descobrir que alguns aplicativos não estão presentes ou não são reconhecidos corretamente. Você pode usar o console de monitoração de licença de software para checar software específico e se necessário adicionar ou corrigir definições de produto.

Escolher quais softwares monitorar

Quando os dados do inventário foi gravado no banco de dados do inventário é exibido no console de SLM sob o modo de exibição **Descoberta**. Você pode selecionar os produtos dessa lista que você quer monitorar e movê-los para o modo de exibição **Monitorado**. Esses produtos podem ser ligados a seus dados de licença e rastreados nos relatórios que mostram como suas licenças correspondem ao uso real do produto. Os produtos que você não deve controlar pode ser movido do modo de exibição **Ignorado** para que saiam do caminho.

Adicionar dados de licença

Você deve adicionar dados sobre as licenças de software que você quer monitorar. É possível adicionar dados manualmente ou importar dados de outra fonte. Após adicionar informações sobre suas licenças, tal como quantas estações você comprou, a data de compra e as datas de vencimento, tipo de licença e como as licenças são consumidas, você verá a estatística de conformidade e relatórios que comparam os dados de licença com uso real de software.

Criar relatório

Ao revisar os dados de software e conformidade de licença você pode gerar um relatório dos dados mostrados no momento. Os relatórios podem ser formatados como arquivos de CSV, HTML, PDF, XML, DOC, XLS ou arquivos de imagem.

Quando você tem licença e dados de software estabelecidos no banco de dados, você também pode usar a ferramenta de relatórios do Management Suite para gerar relatórios de predefinido com licença e dados de uso.

Pré-requisitos para usar o monitoramento de licenças de software

Antes de usar o monitoramento de licenças de software, você deve concluir as tarefas a seguir.

Serviço de inventários configurado e em execução

O monitoramento de licenças de softwares exige que o agente LANDesk esteja em execução nos dispositivos que você quer gerenciar. Depois de obter os dados do inventário, dados do produto são exibidos na tela de produto **Descoberto** do console do SLM. Como a adição de mais dados de inventário, novos dados de produto são adicionados ao modo de exibição **Descoberto** . Isso ocorre no mesmo tempo que a análise de inventário, que por padrão ocorrer uma vez por dia.

Consultas e grupos de dispositivos são definidos

Se você quer controlar softwares nos grupos de computadores (grupo estático) ou usando consultas (grupo dinâmico), crie-os na tela de rede do Management Suite. Os grupos e consultas criados estão disponíveis no console de monitoramento de licença de software. Isto facilitará a revisão dos produtos instalados nos grupos que você organizou por localização, por grupo de empresa, por tipo de hardware, ou outros critérios.

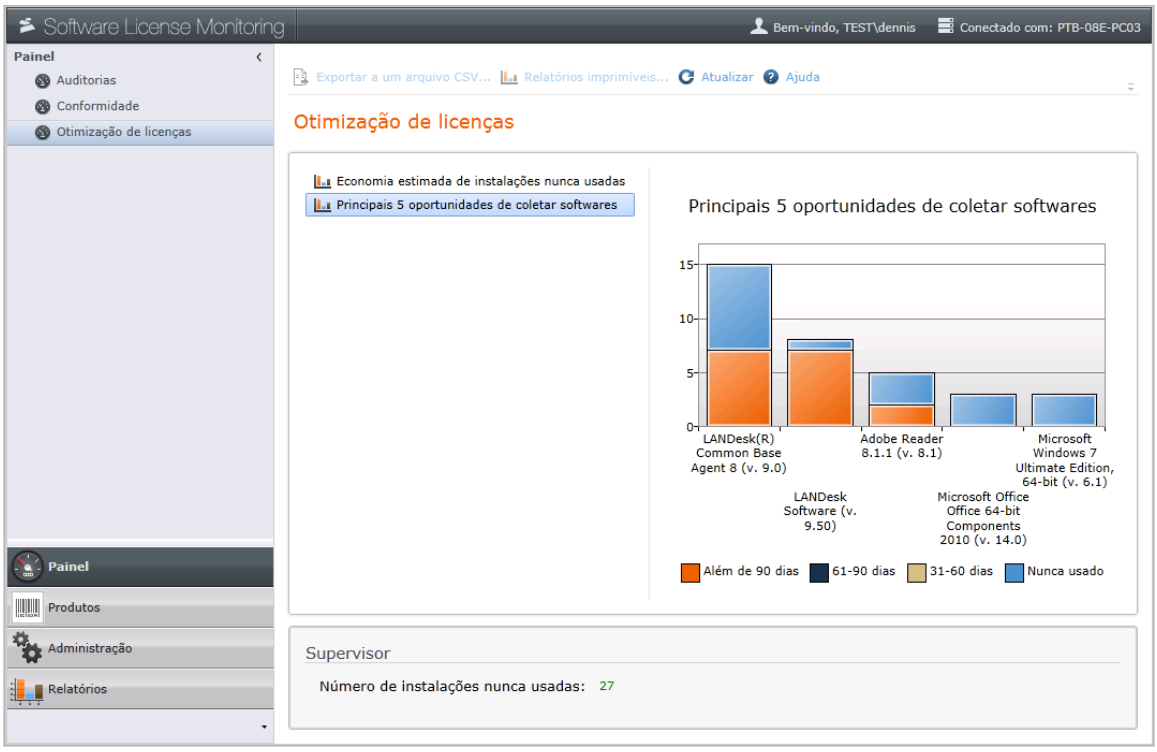
Dados da licença de software disponível

Para monitorar com precisão a conformidade da sua empresa com termos de licença de software, você necessitará de acesso preciso aos dados das licenças. Você pode importar dados para múltiplas licenças ou adiciona licenças individuais como necessário. Quando você estiver certeza que os dados da licença estão corretos, você pode começar a revisar a conformidade usando a ferramenta de monitoramento de licença de software.

Dados de auditoria e de conformidade no dashboard

O dashboard exibe resumos atuais de auditorias importantes e de conformidade de licença. As páginas de dashboard são projetadas dar lhe acesso rápido a dados úteis que é calculado de seu produto e informações de licença.

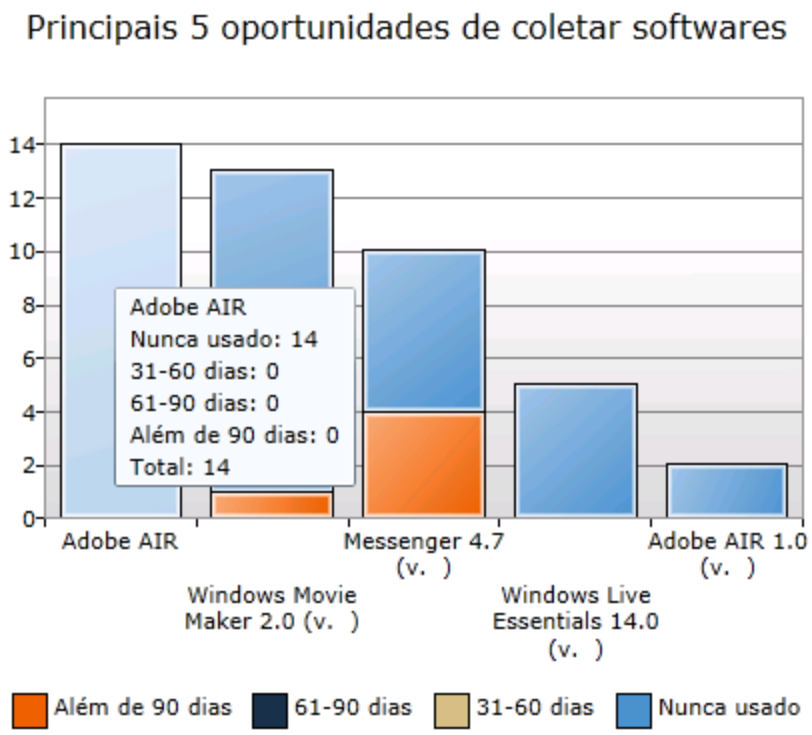
As páginas de dashboard exibem resumos relatórios com mapas e com dados do Auditor. No seguinte exemplo, o mapa exibe as cinco melhores oportunidades de requerer (ou "coletar") as licenças que não estão sendo usadas. A caixa de Auditor no fundo do console mostra o número total de produtos instalados que nunca foram usados.



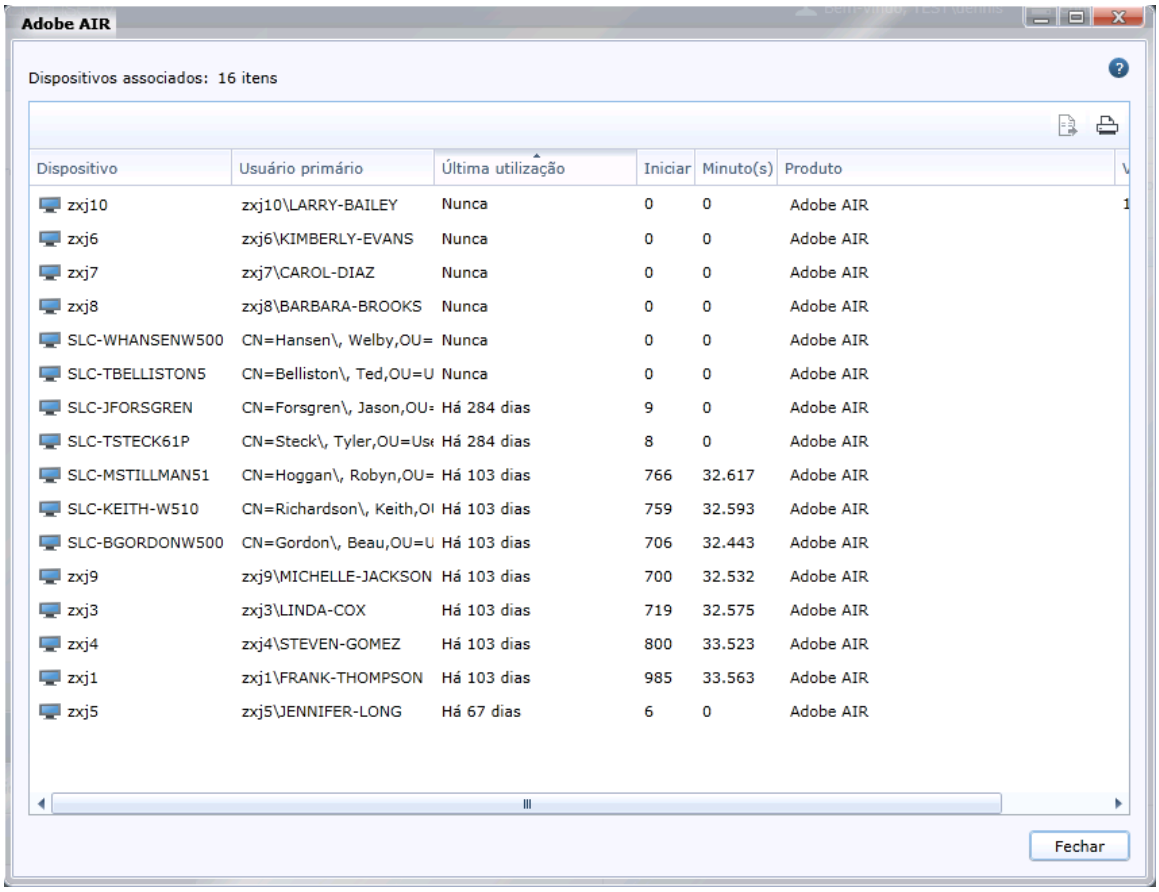
A seção de Auditor fornece um resumo rápido de dados. Os gráficos mostram mais detalhes, e você pode clicar por seções de um mapa ver os detalhes para produtos específicos.

Exibir detalhes do gráfico com tabela

Quando você aponta a uma seção do mapa, uma caixa mostra os dados para essa seção.

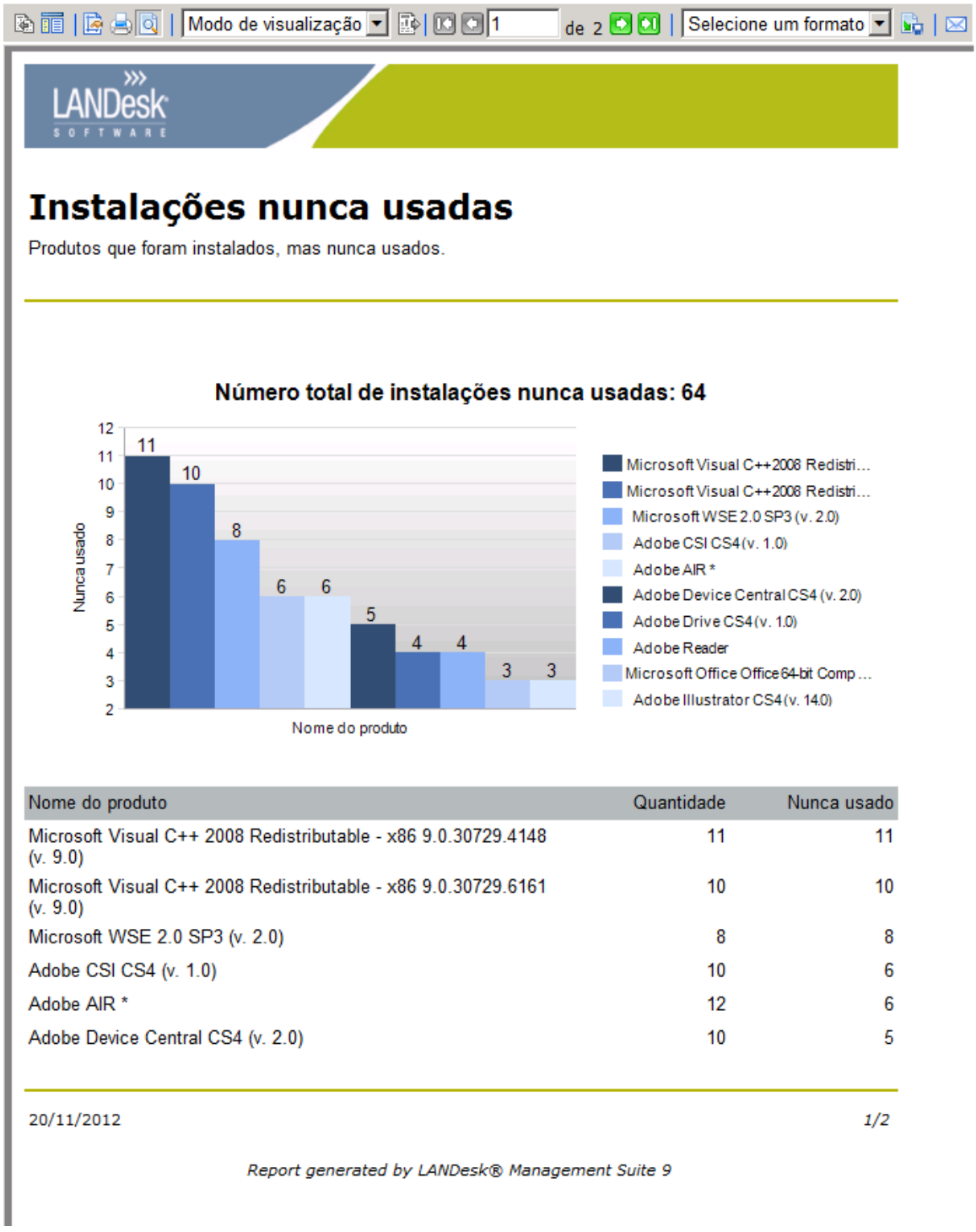


Clique em uma seção de mapa para ver uma lista de dados relacionados. Por exemplo, ao clicar na barra de produto no gráfico de oportunidades de coleta, você verá uma lista de computadores com o produto instalado.


Adobe AIR
Dispositivos associados: 16 itens
Dispositivo
Usuário primário
Última utilização
Iniciar
Minuto(s)
Produto
zxj10 zxj10\LARRY-BAILEY Nunca 0 0 Adobe AIR
zxj6 zxj6\KIMBERLY-EVANS Nunca 0 0 Adobe AIR
zxj7 zxj7\CAROL-DIAZ Nunca 0 0 Adobe AIR
zxj8 zxj8\BARBARA-BROOKS Nunca 0 0 Adobe AIR
SLC-WHANSENW500 CN=Hansen\, Welby,OU= Nunca 0 0 Adobe AIR
SLC-TBELLISTON5 CN=Belliston\, Ted,OU=U Nunca 0 0 Adobe AIR
SLC-JFORSGREN CN=Forsgren\, Jason,OU= Há 284 dias 9 0 Adobe AIR
SLC-TSTECK61P CN=Steck\, Tyler,OU=Us Há 284 dias 8 0 Adobe AIR
SLC-MSTILLMAN51 CN=Hoggan\, Robyn,OU= Há 103 dias 766 32.617 Adobe AIR
SLC-KEITH-W510 CN=Richardson\, Keith,OI Há 103 dias 759 32.593 Adobe AIR
SLC-BGORDONW500 CN=Gordon\, Beau,OU=U Há 103 dias 706 32.443 Adobe AIR
zxj9 zxj9\MICHELLE-JACKSON Há 103 dias 700 32.532 Adobe AIR
zxj3 zxj3\LINDA-COX Há 103 dias 719 32.575 Adobe AIR
zxj4 zxj4\STEVEN-GOMEZ Há 103 dias 800 33.523 Adobe AIR
zxj1 zxj1\FRANK-THOMPSON Há 103 dias 985 33.563 Adobe AIR
zxj5 zxj5\JENNIFER-LONG Há 67 dias 6 0 Adobe AIR
Fechar

Ver detalhes de dados de Auditor

Quando a caixa Auditor conter dados, clique no número para abrir um relatório completo da origem dos dados. No exemplo acima, o Auditor informa que 51 instalações nunca foram usadas. Clique no número 51 abrir um relatório que exposições que produtos são incluído esse total.


Modo de visualização
1
de 2
Selecione um formato
LANDesk
SOFTWARE
Instalações nunca usadas
Produtos que foram instalados, mas nunca usados.
Número total de instalações nunca usadas: 64
Nunca usado
Nome do produto
11
10
8
6
6
5
4
4
3
3
Microsoft Visual C++2008 Redistri...
Microsoft Visual C++2008 Redistri...
Microsoft WSE 2.0 SP3 (v. 2.0)
Adobe CSI CS4 (v. 1.0)
Adobe AIR *
Adobe Device Central CS4 (v. 2.0)
Adobe Drive CS4 (v. 1.0)
Adobe Reader
Microsoft Office Office64-bit Comp...
Adobe Illustrator CS4 (v. 14.0)
Nome do produto | Quantidade | Nunca usado
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4148 (v. 9.0) | 11 | 11
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161 (v. 9.0) | 10 | 10
Microsoft WSE 2.0 SP3 (v. 2.0) | 8 | 8
Adobe CSI CS4 (v. 1.0) | 10 | 6
Adobe AIR * | 12 | 6
Adobe Device Central CS4 (v. 2.0) | 10 | 5
20/11/2012
1/2
Report generated by LANDesk® Management Suite 9

Exportar dados para CSV e relatórios

Ao clicar em um gráfico para exibir detalhes dos dados, ou a qualquer momento que estiver na tela de detalhes de produto, você pode exportar dados como um arquivo de CSV ou criar um relatório.

Para exportar dados em formato de CSV

1. Clique uma seção de um mapa.
2. Na nova janela, selecione os dispositivos que você quer incluir nos dados exportados. (Clique na lista e pressione **Ctrl+A** para selecionar todos os dispositivos).
3. Clique em **Exportar** .
4. Especifique a localização para salvar o arquivo de CSV em e clique em **Salvar**.

Para criar um relatório de dados selecionados

1. Clique uma seção de um mapa.
2. Na nova janela, selecione os dispositivos que você quer incluir no relatório. (Clique na lista e pressione **Ctrl+A** para selecionar todos os dispositivos).
3. Clique em **Relatório** .
4. Na barra de ferramentas da tela de relatório, selecione um formato salvar o relatório e clique no botão **Exportar** .
5. Especifique o local onde salvar o relatório e clique em **Salvar**.

Exibição do dashboard de auditorias

A página de Auditorias do dashboard inclui relatórios que são útil quando você prepara para uma auditoria de seu uso de licença de software.

Relatório: Total de instalações principais

Este relatório lista os cinco produtos com as a maioria de instalações em computadores em sua empresa. Isso conta as instalações reais, não o número de dispositivos, porque você pode ter mais de uma instalação em um dispositivo.

Supervisor: Produtos e licenças com sinalizadores de auditoria:

Este relatório alerta para assuntos que poderiam ser destacados durante uma auditoria de licença de software. Estes incluem problemas com documentação de licença e produtos que não foram distribuídos (movidos para os grupos Monitorados ou Ignorados). O Auditor conta itens como:

- Licenças sem uma ordem de compra
- Produtos sem licenças
- Produtos descobertos que não foram dispostos
- Licenças sem nota fiscal do fabricante

Clique em um número para qualquer item ver um relatório pleno desse item.

NOTA: Você também achará relatórios de predefinido para itens individuais de bandeira de auditoria na ferramenta de Relatórios de SLM.

Exibição do dashboard de conformidade

A página de Conformidade do dashboard inclui relatórios que exibem os produtos fora de conformidade com termos de licença e necessita sua atenção. Isto inclui uma estimativa do custo de conformidade de todos os produtos instalados para que todos os produtos tenham licenças válidas.

Relatório: Principais fora de conformidade por instalação

Este mapa mostra até cinco produtos que têm o mais alto número de instalações ilícitas.

Relatório: Principais não em conformidade por custos ajustados

Este mapa mostra os produtos que têm o mais alto custo trazê-los em conformidade. Isto é determinado pelo número de instalações sem licença multiplicado pelo custo unitário associado ao produto.

Relatório: Principais não em conformidade por fabricante

Este mapa agrupa produtos por fabricante e exposições que os produtos do fabricante tem as instalações mais ilícitas. Isto é útil identificar necessidades de conformidade quando você tem uma auditoria com um fabricante e necessidade verificar-se que instalação combina os termos de sua licença para esse fabricante.

Supervisor: Custo estimado de conformidade:

O custo estimado total para que os produtos instalados estejam em conformidade com os requisitos de licença. Isto é determinado pelo número de instalações sem licença multiplicado pelo custo unitário associado ao produto.

Supervisor: Produtos fora de conformidade

O número de produtos que não estão em conformidade com licenças associadas. Clique no número para ver uma lista completa de produtos que são para fora de conformidade.

Exibição do dashboard de otimização de licenças

A página de Otimização de licença do dashboard inclui relatórios que calculam a economia que você pode ter removendo softwares não usados de computadores em sua empresa. Estes relatórios focam em software instalado que nunca foi usado nem não foi usado para um comprimento especificado de tempo.

NOTA: Os produtos são considerados "nunca usados" quando um valor de 0 é retornado nos dados de inventário para a quantia de tempo que o produto foi executado. No entanto, é possível que um produto esteja instalado e a pessoa usando só tenha iniciado o aplicativo uma vez e encerrou em menos de um minuto. Neste caso, o produto ainda será exibido como "nunca usado" no dashboard e em relatórios.

Relatório: Economia estimada de aplicativos nunca usados

Este relatório lista os cinco produtos nunca-usados que mais economizariam caso sejam removidos. Isto é baseado no número de instalações nunca-usados de produto multiplicadas pelo custo unitário associou-se com o produto.

Relatório: Principais 5 oportunidades de coletar softwares

Este relatório lista os cinco produtos com o mais alto número de instalações de produto nunca-usados ou infreqüentemente usadas. Não calcula custos, mas lista o número de computadores com cada produto que não usou o produto dentro de um certo número de dias (31-60, 61-90, acima de 90 e nunca usado).

Supervisor: Número de instalações nunca usadas:

Este relatório soma o número de exemplos em que instalou software nunca foi usado. O relatório lista cada produto com o número total de instalações e quantas vezes o produto não foi usado.

Monitoração de uso de software

A análise de monitoramento de software do LANDesk Management Suite é executado quando você agenda análises de inventário regulares. Ela monitora arquivos executáveis em execução e compara as informações do aplicativo em cada dispositivo com nomes os nomes e tamanhos dos arquivos executáveis armazenados no banco de dados.

Dua outras análises de inventário ajuda a completar a imagem com outros dados sobre software. Essas análises examinam o registro do Windows, chaves de remoção, arquivos .msi, atalhos e GUIDs para identificar produtos de software. Todos os dados de análise são comparados para dar uma imagem completa do software instalado em cada dispositivo gerenciado.

O console de monitoramento de licença de software exibe este resumo de dados no modo de exibição de Produtos. Ainda que você não tenha dados de licença disponíveis, você pode ver este dados de produto para descobrir em quantos dispositivos gerenciados um produto de software foi descoberto.

Monitorar e ignorar produtos

Quando você primeiro abre o console do SLM, todos produtos recentemente descobertos são achados no modo de exibição **Descoberto** de produto. Ao gerenciar o uso de softwares e licenças, você pode escolher qual software é importante para monitoramento. O software que você quer rastrear pode ser movido para o modo de exibição de produto **Monitorado**. Alguns softwares não precisam ser importantes para você, você pode move-los para o modo de modo de exibição de produto **Ignorado**, removendo-os do cálculo de conformidade de licença.

Para monitorar um produto de software

1. Clique em **Produtos > Descoberto**.
2. Use a caixa de **Pesquisa** para achar o produto.
3. Clique no botão. Na barra de ferramentas, clique **Ações > Mover para> Controlado**s.

O produto agora é listado no modo de exibição produtos **Monitorados**.

NOTA: Você também pode clicar com o botão direito em um produto e selecionar **Mover para > Monitorados**.

Para ignorar um produto ou o grupo de produtos de software

1. Clique em **Produtos > Descobertos**.
2. Use a caixa de **Pesquisa** para achar o produto.

3. Clique no botão. Na barra de ferramentas, clique **Ações> Mover para> Ignorados**.

O produto agora é listado no modo de exibição **Ignorada** de produto.

NOTA: Você também pode clicar com o botão direito em um produto e selecionar **Mover para > Ignorados**.

Localizar um produto

No modo de exibição de Produtos, uma caixa de pesquisa ajuda a localizar produtos mais rapidamente. Você pode pesquisar com um mínimo de dois caracteres, exibindo resultados que correspondem ao string nas colunas de Produtos ou Fabricantes.

Usar a caixa de Pesquisa para localizar um produto

1. Clique em **Produtos** e abra um dos modos de exibição (Monitorado, Descoberto, Ignorado ou Todos).
2. Na caixa de **Pesquisa**, digite pelo menos dois caracteres e pressione **Enter**.

   A lista contém todos os produtos ou fabricantes com a string inserida.
3. Selecionar um ou mais itens da lista e clique no botão da barra de ferramentas ou clique com o botão direito nos itens para executar alguma ação. Você pode arrastar os itens para outra exibição para move-los.
4. Para visualizar todos os produtos na lista novamente, clique no **X** da caixa de pesquisa para limpar a pesquisa.

Pesquisa avançada de produtos

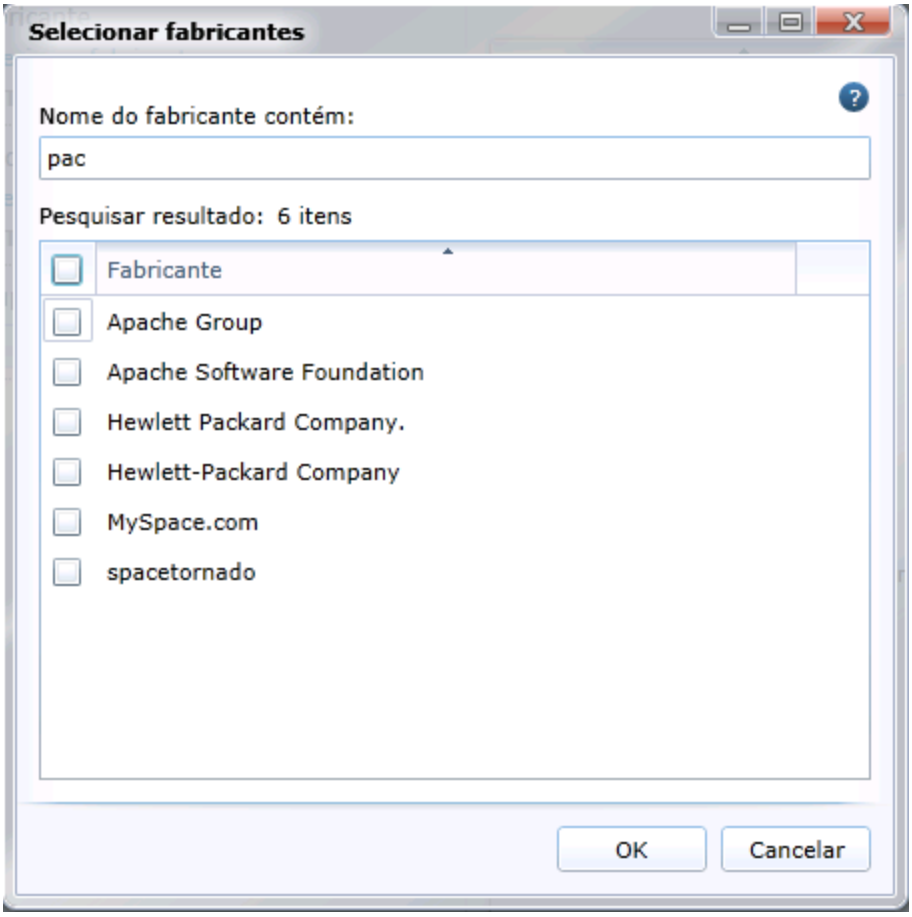
Filtre uma lista de exibição de produto selecionando um fabricante, produto ou grupo de computadores como filtro. Você pode usar um ou mais desses filtros para exibir um número menor de produtos na lista. Esses filtros são encontrados na coluna a esquerda da lista de produtos.

- Selecionar um **fabricante** (ou fabricante normalizado) para exibir somente produtos que estão associados com o fabricante.
- Selecionar um **produto** (ou produto normalizado) para exibir somente produtos que correspondem um nome do produto.

- Selecionar um **grupo de computadores** para exibir somente os produtos que estão instalados em computadores daquele grupo. Isso é útil para achar produtos quando você sabe que eles estão instalados em um certo grupo de computadores na sua organização.

Filtrar uma pesquisa de produto por fabricante

1. Clique em **Produtos** e abra um dos modos de exibição (Monitorado, Descoberto, Ignorado ou Todos).
2. Na coluna a esquerda da lista, clique **Selecionar fabricantes.**
3. Digite pelo menos três caracteres na caixa de nome de fabricante. Nomes correspondentes são listados na caixa **Resultados da pesquisa.**

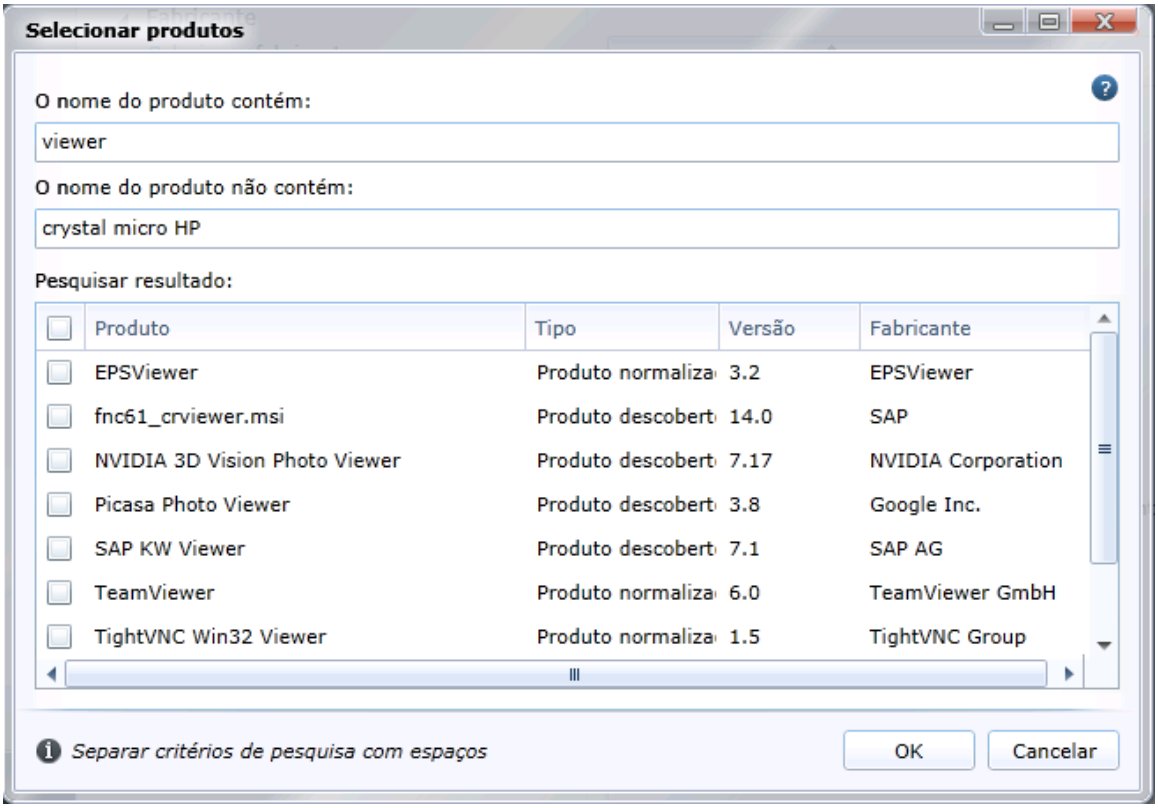


4. Selecionar os nomes dos fabricantes que você quiser usar como filtros, depois clique em **OK.**

Filtrar uma pesquisa de produto por nome

1. Clique em **Produtos** e abra um dos modos de exibição (Monitorado, Descoberto, Ignorado ou Todos).
2. Na coluna a esquerda da lista, clique **Selecionar produtos.**

3. Digite pelo menos três caracteres na caixa de nome do produto. Nomes correspondentes são listados na caixa **Resultados da pesquisa.** Você também pode especificar strings para excluir dos resultados de busca. Para fazer isso, digite um ou mais strings separados com um espaço na caixa **Nome do produto não contém**. Isso pode ajudar a reduzir o números de resultados da pesquisa.



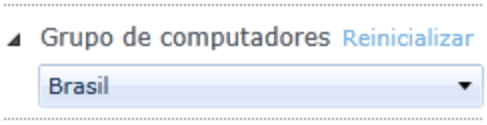
4. Selecionar os nomes dos produtos que você quer usar como filtros e clique em **OK.**

Filtrar uma pesquisa de produtos por grupo de computadores

1. Clique em **Produtos** e abra um dos modos de exibição (Monitorado, Descoberto, Ignorado ou Todos).
2. Na coluna à esquerda da lista, clique na lista **Grupo de computadores** e selecione um grupo de computadores.

A lista muda para exibir somente os produtos instalados nos computadores no grupo que você selecionou.

3. Para remover os filtro e visualizar todos os produtos, clique em **Redefinir.**



Exibir todos os produtos instalados

Depois que você separar os produtos em "monitorados" e "ignorados", você pode necessitar achar um produto mas não se lembra em que grupo. Você pode procurar por todos os produtos que foram descobertos usando o modo de exibição de **Todos os produtos instalados**.

Para ver todos produtos instalados

1. Clique em **Produtos**.
2. Clique em **Todos os produtos instalados**
3. Use a caixa de pesquisa ou filtros para achar o produto que você quer.
4. Para determinar qual modo de exibição de produto contém o produto, olhar na coluna **Status**. Isto mostra se o produto é monitorado, é descoberto, ou é ignorado.

Criar produtos personalizados

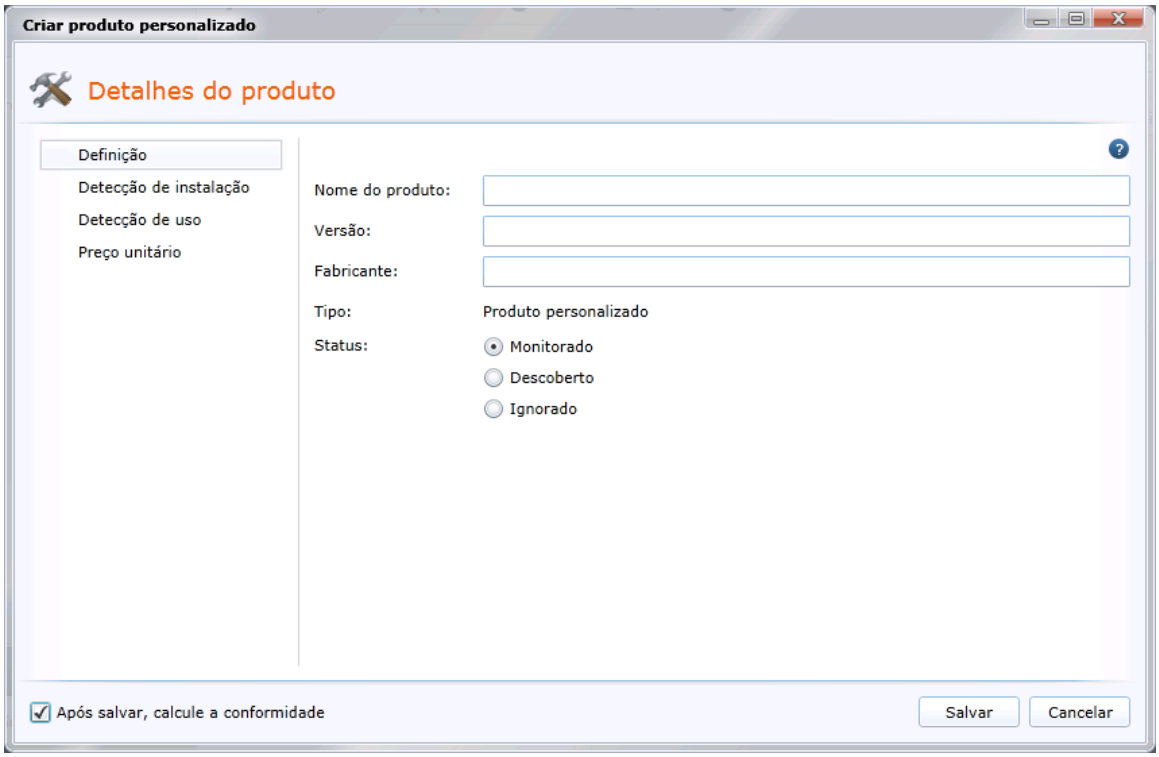
Você pode criar produtos personalizados para qualquer arquivo executável de software não identificado ou identificado erroneamente. Ao fazer isto, os arquivos do produto personalizado são adicionados à lista de arquivos que o analisador de inventário procurará.

Você pode especificar quais arquivos indicam que o software foi instalado, e também especifica arquivos de uso que indicam quando o software é executado em um computador.

Em alguns casos você pode querer usar uma consulta Management Suite para encontrar produtos instalados. Você faria isto quando um produto não é identificado corretamente a partir dos arquivos executáveis mas pode ser identificado com base em dados de estoque que você pode adicionar a uma consulta.

Para criar uma definição personalizada de produto

1. Clique em **Produtos** e em exibir no modos de exibição de produtos.
2. Na barra de ferramentas, clique **Novo > Produto personalizado**.



3. Digite o nome no campo **Nome do produto**.
4. Digite um número ou número com um caractere curinga no campo **Versão**.
5. Digite ao menos três caracteres no campo **Fabricante** para exibir os nomes correspondentes. Selecione o nome de fabricante.
6. Em **Status**, selecione **Monitorados** ou **Ignorados** para listar este novo produto em um dos modos de exibição do produto. (Por padrão, um produto personalizado é movido aos produtos monitorados).
7. Clique em **Detecção de instalação**.

8. Se quiser detectar produtos baseados em uma consulta do Management Suite selecione **Usar detecção de consulta**. Clique em **Navegar** e selecione uma consulta que você criou na tela de rede do Management Suite. Todos os dispositivos que correspondem a consulta serão retornados como tendo uma correspondência para este produto.
9. Selecione **Usar detecção de arquivo** para detectar produtos baseados em arquivos instalados. Os nomes de arquivo que você adicionar aqui determinam como o produto será detectado durante a análise do inventário.
10. Clique no botão **Adicionar (+)**. Na caixa de diálogo **Adicionar arquivos**, você pode selecionar um nome de arquivo existente (um que existe no banco de dados de inventário), ou você pode clicar em **Definir novo arquivo** e especificar o nome de arquivo, tamanho do arquivo, e número de versão para o arquivo de produto. Repita isto para cada arquivo de produto que você quer usar. Ao terminar, clique em **OK**.
11. Selecione **Corresponder todos** ou **Corresponder qualquer um** para especificar se todos ou pelo menos um arquivo precisa ser encontrado.
12. Clique **Detecção de uso**. Use esta opção para incluir arquivos que indicam o produto está sendo usado.
13. Clique no botão **Adicionar (+)**. Na caixa de diálogo **Adicionar arquivo**, você pode selecionar um nome de arquivo existente (um que existe no banco de dados de inventário), ou você pode clicar em **Definir novo arquivo** e especificar o nome de arquivo, tamanho do arquivo, e número de versão para o arquivo de produto. Repita isto para cada arquivo de produto que você quer usar. Ao terminar, clique em **OK**.
14. Clique em **Preço unitário**. Selecione um método para calcular o preço unitário:
    - Selecione **Uso preço unitário** automaticamente calculado se você tem múltiplas licenças para o produto com preços unitários diferentes. Se você selecionar esta opção, o preço unitário é uma média de todos os preços unitários das licenças diferentes.
    - Selecione **Especificar um preço unitário** se você quer usar o mesmo preço unitário para todos os cálculos. Por exemplo, se você tem duas licenças com preços unitários diferentes para o mesmo produto e você quer usar o preço mais alto para cálculos, você pode especificar que preço unitário aqui.
15. Se você adicionar informações de produto que afetarão a licença e os cálculos de uso, como quando um produto é associado com uma licença monitorada, selecione **Calcular conformidade após salvar** para iniciar o cálculo novamente e manter os relatórios de conformidade atualizados.
16. Quando todas as informações estiverem completas, clique em **Salvar**.

IMPORTANTE: Os dois tipos de arquivos de detecção, instalação e uso, são necessários para reunir dados de produto em análises de inventário. Os arquivos de instalação indicam que um arquivo foi instalado e é necessário determinar quando um produto de software existe num computador. Arquivos de uso indicam que o software foi executado e são necessário para determinar se o produto instalado foi usado.

Se um inventário do computador exibe uma correspondência para os arquivos de instalação, o SLM informará que o software foi instalado. No entanto, se não houver nenhum arquivo de uso especificado para o produto, o SLM sempre informará que o software nunca foi usado. Quando você criar um produto personalizado, você deve certificar-se de definir ao menos um arquivo de uso para que o SLM informe com precisão se or produto foi usado.

Editar um produto descoberto

1. Clique em **Produtos > Descobertos**.
2. Ache o produto usando a caixa de **Pesquisa** ou o filtro **Selecionar produtos**.
3. Selecione um o produto e clique no botão **Editar** na barra de ferramentas.

   A caixa de diálogo **Editar detalhes do produto** abre; alguns itens são somente-leitura e outros são editáveis.
4. Em **Status**, selecione **Monitorados** ou **Ignorados** para listar este novo produto em um dos modos de exibição do produto.
5. Clique em **Detecção de instalação**. Todas as opções são somente-leitura.
6. Clique **Detecção de uso**. Você pode adicionar arquivos que indicam o produto está sendo usado.
7. Clique no botão **Adicionar (+)**. Na caixa de diálogo **Adicionar arquivos**, você pode selecionar um nome de arquivo existente (um que existe no banco de dados de inventário), ou você pode clicar em **Definir novo arquivo** e especificar o nome de arquivo, tamanho do arquivo, e número de versão para o arquivo de produto. Repita essas etapas para cada arquivo que quiser usar para determinar quando o produto está em uso. Ao terminar, clique em **OK**.
8. Clique em **Preço unitário**. Se as opções podem ser editadas, você pode mudar o preço unitário que é usado para calcular custos relacionados a trazer licenças em conformidade.
9. Quando todas as informações estiverem completas, clique em **Salvar**.

Criar produto normalizado

Ao revisar os dados do produto, você pode descobrir que o mesmo produto é representado por múltiplas instâncias do produto e número da versão. Você pode normalizar os produtos para que o nome do produto e número da versão sejam usados no lugar de todas as variações do produto e versão.

Por exemplo, computadores na sua organização podem ter múltiplas versões do Adobe Reader instalados. Se você tiver interesse em acompanhar números de versões antigas separadamente, selecione todas as instâncias do Adobe Reader 7, 8 e 9 no modo de exibição de Produtos **Descobertos** e padronize como "Adobe Reader". Se você quiser rastrear quantos computadores têm a versão X instalada, selecione todas as instâncias do Adobe Reader X (como o número da versão 10.0 e 10.1) e padronize como "Adobe Reader X".

Um produto normalizado fica em exibição com um sinal de mais (+) antes do nome do produto. Clique no sinal de mais para expandir o produto e ver todas as variações incluídas.

Produto	Versão	Instalado	Não licenciado	Nunca usado	Noventa dias sem uso	Fabricante	Status
Adobe AIR	--	22	--	21	1	Adobe*	Monitorado
Adobe AIR	2.5	4	--	4	0	Adobe Systems Inc.	Contido
Adobe AIR	2.7	7	--	6	1	Adobe Systems Incorporated	Contido
Adobe AIR	3.0	2	--	2	0	Adobe Systems Incorporated	Contido
Adobe AIR	1.5	1	--	1	0	Adobe Systems Inc.	Contido
Adobe AIR	2.0	1	--	1	0	Adobe Systems Inc.	Contido
Adobe AIR	1.1	1	--	1	0	Adobe Systems Inc.	Contido
Adobe AIR	2.6	6	--	6	0	Adobe Systems Incorporated	Contido
Adobe Reader	--	10	--	1	9	Adobe Systems Incorporated	Monitorado
Adobe Reader X	--	21	--	0	21	Adobe Systems Incorporated	Monitorado

Criar um produto normalizado

1. Clique em **Produtos** e em um dos modos de exibição do produto (Monitorado, Descoberto, Ignorado ou Todos os produtos instalados).
2. Encontre os nomes dos produtos que você deseja combinar, usando a caixa de **Pesquisa**.
3. Selecione os nomes de produtos e depois clique em **Ações > Grupo**.
4. Edite o nome que deseja usar como nome de produto normalizado.
5. Selecione em qual status você deseja que o produto esteja listado (**Monitorado** ou **Ignorado**).
6. Clique em **Salvar**.

O nome selecionado aparecerá na exibição de produto que você selecionou. Um sinal de mais (+) ao lado do nome indica que é um produto normalizado. Quando você abrir o nome (clique +) você verá que todos os nomes estão agrupados para aquele nome normalizado.

Para adicionar automaticamente os produtos para um produto normalizado

1. Clique em **Produtos** e depois clique em uma das exibições de produto (Monitorado, Descoberto, Ignorado ou Todas).
2. Clique **Novo > Produto normalizado** na barra de ferramentas. (se desejar adicionar produtos a um produto normalizado existente, selecione o produto e clique em **Editar** na barra de ferramentas.)
3. Digite o nome que deseja usar como nome de produto normalizado.
4. Selecione em qual status você deseja que o produto esteja listado (**Monitorado** ou **Ignorado**).
5. Clique em **Regras dinâmicas.**
6. Digite uma regra na caixa. Use um asterisco (*) como curinga.
7. Para adicionar outra regra, clique o **Adiciona** botão de [+] e bata outra regra.
8. Quando todas as regras forem adicionadas, clique em **Salvar**.

Os atuais nomes de produtos no banco de dados que correspondem às regras estão listados na caixa **Produtos coincidentes**. Enquanto novos dados de inventário são adicionados e outros nomes de produtos são adicionados ao banco de dados, esses nomes serão incluídos automaticamente no produto normalizado.

NOTA: Com alguns produtos normalizados você pode especificar um único nome de fabricante na página **Definição.** Entretanto, alguns nomes normalizados incluem produtos com diferentes variações do nome do fabricante. Se este for o caso, use uma string parcial com um parcial de partida com um coringa para que todas as variações sejam incluídas. Por exemplo, digite **Adobe*** na caixa do fabricante para incluir todas as variações do "Adobe Systems" como fabricante.

Excluir um produto normalizado

Você pode excluir um produto normalizado selecionando-o e pressionando a tecla **Excluir.** Se você fizer isso, os produtos individuais que estavam agrupados voltarão para a lista de produtos como produtos individuais.

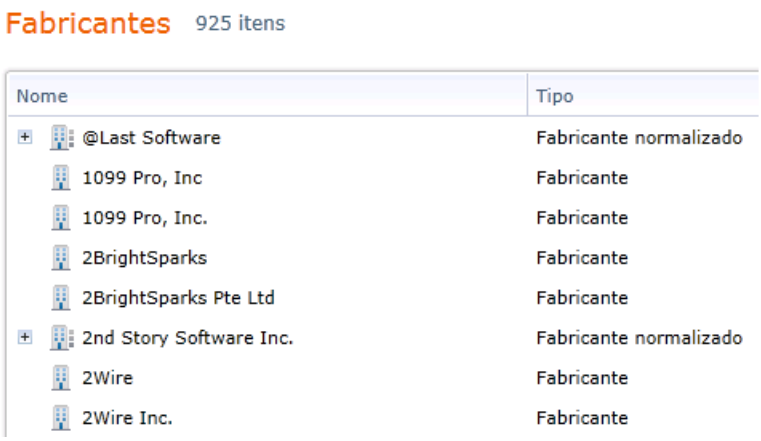
Se você apagar um produto normalizado, qualquer licença associada com aquele produto não será mais associada com ele, e relatórios de conformidade não irão mais mostrar o produto normalizado como licença de consumo. Quando isso acontece você deveria editar as licenças e revisar as associações dos produtos para cada licença.

Criar um fabricante normalizado

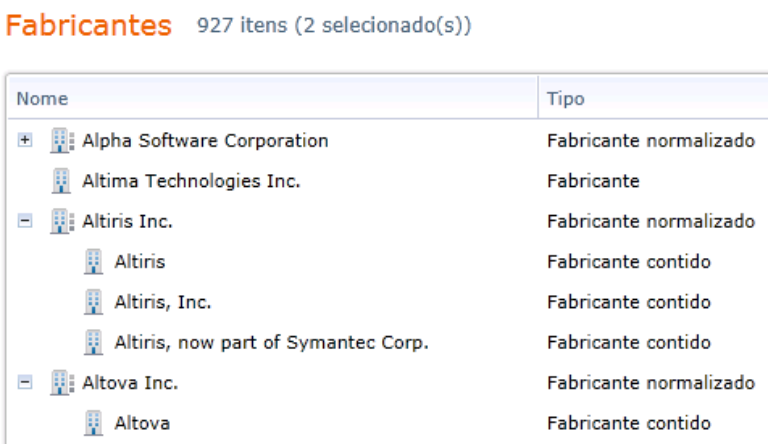
Ao adicionar dados do inventário à monitoramento da licença de software, você pode encontrar variações para o nome de uma mesma empresa. Você pode criar um nome normalizado de fabricante que é usado em lugar de todas as variações dos nomes de fabricante.

Nomes de fabricantes normalizados são precedidos de um sinal de mais (+) na lista.

Por exemplo, na lista a seguir existem quatro variações do fabricante do software Alchemy:



Você pode selecionar esses nomes e agrupa-os de modo que um nome normalizado seja usado para todos eles. Que o nome normalizado seja exibido na lista.



Fabricantes normalizados fornecidos com este produto

Este produto inclui fabricantes normalizados. A primeira vez que você abre a lista de fabricantes, você notará que a lista inclui nomes de fabricante geralmente usados que foram normalizados.

O LANDesk pode fornecer fabricantes normalizados adicionais. Quando estiverem disponíveis, o download como conteúdo de patch será feito automaticamente. Se você já definiu fabricantes normalizados, seu conteúdo será mantido. Qualquer novos fabricantes normalizados que talvez discordem com o próprias definições não substituirão seu conteúdo personalizado.

Defina um fabricante normalizado

Você pode definir um fabricante normalizado nas seguintes maneiras.

Para criar um fabricante normalizado

1. Clique em **Administração> Fabricantes**.
2. Ache os nomes de fabricante que você quer combinar (usando a caixa de **Pesquisa** se necessário).
3. Selecione os nomes de fabricante que você quer incluir no nome normalizado.
4. Clique **Ações > Grupo**.
5. Selecione o nome que você quer usar como o nome normalizado de fabricante. (Você deve selecionar um dos nomes existentes).
6. Clique em **OK**.

O nome que você seleciona é adicionado aos nomes normalizados de fabricante nos Fabricantes lista. Ao abrir o nome (clique +) você verá que todos os nomes estão agrupados para aquele nome padronizado.

Para adicionar automaticamente os fabricantes a um produto normalizado

Você pode criar regras que automaticamente adicionarão qualquer nomes de fabricante a um nome normalizado. Por exemplo, você podia especificar que qualquer nome de fabricante que começa com " Adobe Sys*" automaticamente é adicionado ao nome normalizado " Adobe Sistemas Incorporated".

1. Clique em **Administração> Fabricantes**.
2. Na barra de ferramentas, clique **Novo > Fabricante**.
3. Digite o nome do fabricante normalizado.
4. Clique em **Regras dinâmicas.**
5. Digite uma regra na caixa. Use um asterisco (*) como curinga.
6. Para adicionar outra regra, clique o **Adiciona** botão de [+] e bata outra regra.
7. Ao terminar, clique em **Salvar**.

Os atuais nomes de fabricantes no banco de dados que correspondem às regras estão listados na caixa **Fabricantes coincidentes**. Enquanto novos dados de inventário são adicionados e outros nomes de fabricantes são adicionados ao banco de dados, esses nomes serão incluídos automaticamente no produto normalizado.

Para adicionar um nome de fabricante a um fabricante normalizado existente

Se você criou um fabricante normalizado e encontrar outro nome de fabricante que quer incluir com outros nomes, você pode adicionar o nome ao nome normalizado.

1. Clique em **Administração> Fabricantes**.
2. Selecione o nome de fabricante que você quer adicionar ao nome normalizado de fabricante.
3. Clique **Ações > Mover para fabricante normalizado**.
4. Selecione um fabricante normalizado e clique em OK.

Monitoramento de produtos da Web

Você pode controlar aplicativos baseados na Web da mesma forma que você controla o software instalado em um dispositivo. Para controlar estes tipos de produtos no console do SLM, você crie produtos de Web.

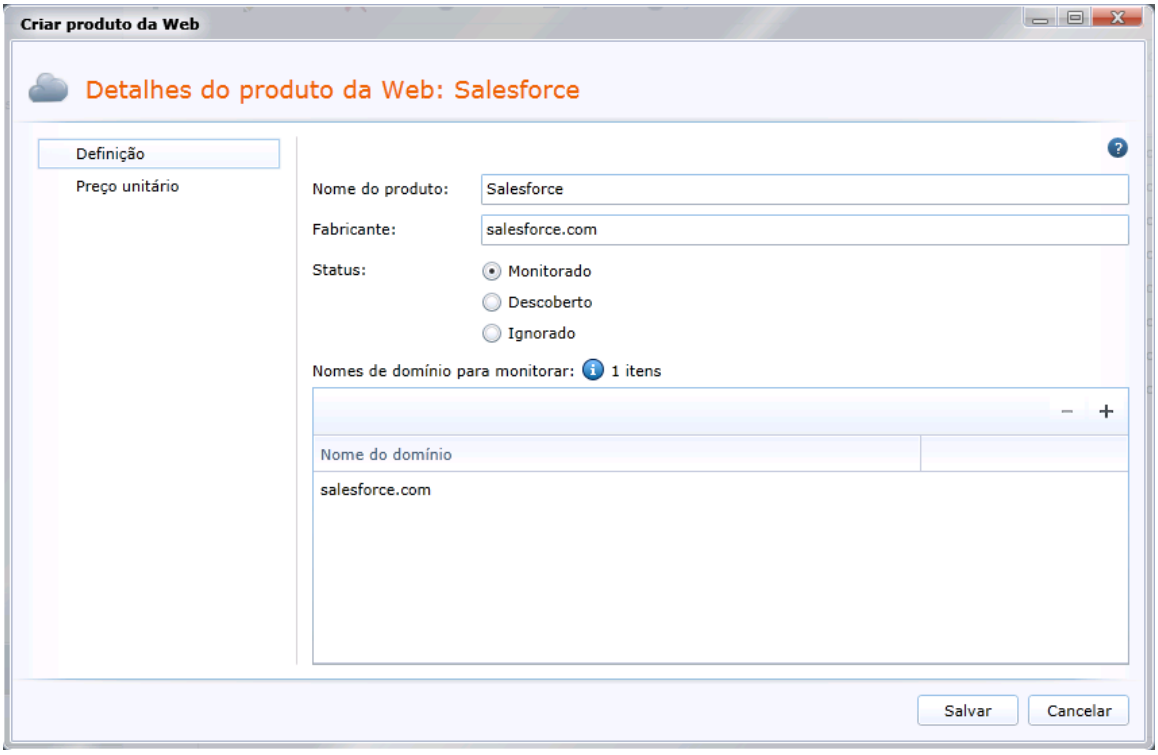
Quando você cria um produto de Web no console do SLM, você especifica a qual o URL o produto é associado. Este URL é adicionado à lista de itens que o analisador de inventário pesquisa nos dispositivos gerenciados. Você só deve especificar um domínio superior; nenhum caminho, número de porta nem de página no domínio podem ser especificados. Você pode adicionar subdomínios.

O analisador de inventário pode rastrear quais dispositivos acessam a URL e por quanto tempo. Esses dados são incluídos em relatórios de monitoramento de software e cálculos.

Por exemplo, se você usasse Salesforce para rastrear vendas e serviço de cliente, você definiria um produto chamado "Salesforce" e associa-se-o com o URL para que é acessado faz logon.

Defina um produto da Web

1. Clique em **Produtos > Monitorados**.
2. Na barra de ferramentas, clique em **Novo > Produto da Web**.



3. Digite o nome na caixa de **Nome de produto** .
4. Digite ao menos três caracteres no campo **Fabricante** para exibir os nomes correspondentes. Selecione o nome de fabricante. Se não há nenhuma partida, bata o nome pleno de fabricante na caixa.
5. Em **Status**, selecione **Monitorados** ou **Ignorados** para listar este novo produto em um dos modos de exibição do produto.
6. Em nomes **Nomes de domínio para monitorar**, clique no botão **Adicionar (+)**.
7. Digite o nome de domínio para o produto de Web.
8. Clique em **Preço unitário**. Selecione um método para calcular o preço unitário:

- Selecione **Uso preço unitário** automaticamente calculado se você tem múltiplas licenças para o produto com preços unitários diferentes. Se você selecionar esta opção, o preço unitário é uma média de todos os preços unitários das licenças diferentes.
- Selecione **Especificar um preço unitário** se você quer usar o mesmo preço unitário para todos os cálculos. Por exemplo, se você tem duas licenças com preços unitários diferentes para o mesmo produto e você quer usar o preço mais alto para cálculos, você pode especificar que preço unitário aqui.

9. Quando todas as informações estiverem completas, clique em **Salvar**.

Exibir todos os dispositivos com um produto instalado

Ao ver uma lista de nomes de nomes de produto ou em gráficos no dashboard, você pode exibir uma lista de todos os dispositivos com um produto instalado.

Ao ver a lista de dispositivos, você pode criar um relatório próprio para impressão da lista ou exportar os dados como arquivo CSV para sua referência.

Para ver dispositivos de um produto em uma lista de produto

1. Clique em **Produtos** e em uma das exibições de produto (Monitorado, Descoberto, Ignorado ou Todos os produtos instalados).
2. Ache o produto usando a caixa de **Pesquisa** ou em **Selecione produtos**.
3. Clique duas vezes no nome do produto.

   Uma lista de dispositivos é exibida numa nova janela.
4. Para exportar uma lista de dispositivos em formato de CSV, selecione os dispositivos e clique o botão **Exportação** .
5. Para criar um relatório dos dispositivos, clique o botão **Relatório** .

Para ver dispositivos de um produto em um gráfico no dashboard

1. Clique em **Dashboard** e selecione uma das opções de dashboard (Auditorias, Conformidade ou Otimização de licenças).
2. Clique em um segmento de um mapa que representa um produto.

   Uma janela separada abre com uma lista de dispositivos.
3. Para exportar uma lista de dispositivos em formato de CSV, selecione os dispositivos e clique o botão **Exportação** .
4. Para criar um relatório dos dispositivos, clique o botão **Relatório** .

Reiniciar o cálculo de uso de um produto

Normalmente, o uso do produto é calculado da primeira vez que um produto é encontrado na análise do inventário. Com o correr do tempo pode haver situações onde você precisará fazer o cálculo para obter uma imagem mais precisa do uso atual do produto.

Por exemplo, se um produto foi instalado por vários meses e usou algumas vezes em alguns computadores, você pode redefinir o cálculo de uso de produto para esse produto. Após fazer isso, os novos dados de uso (número de inícios e minutos usados) refletirão apenas o uso da vez que você o reiniciou.

NOTA: Mantenha em mente que quando você redefine o cálculo de uso do produto, as informações existentes de uso de produto para esse produto serão retiradas do banco de dados.

Para reiniciar o cálculo de uso de um produto

1. Clique na guia **Produtos** e clique em uma das exibições de produto (Monitorado, Descoberto, Ignorado ou Todos os produtos instalados).
2. Ache o produto usando a caixa de **Pesquisa** ou em **Selecione produtos**.
3. Clique com o botão direito no produto e selecione **Redefinir uso do produto.**
4. Clique em **OK** para confirmar que você quer excluir as informações.

Especifique arquivos para detectar a instalação e uso do produto

Há duas maneiras de determinar se um produto está instalado e sendo usado num dispositivo gerenciado. O analisador de inventário identifica dois tipos de arquivos:

- Os arquivos que indicam o produto foram instalados
- Os arquivos que indicam o produto foram usados

Os arquivos são definidos por nome do arquivo, número de versão, e tamanho (em bytes). Produtos automaticamente descobertos também excepcionalmente são identificados pelo GUID associou-se com o produto, que é por que aí podem aparecer estar duplicatas de um produto. Dois produtos podem compartilhar um nome semelhante e versão mas tem GUIDs diferente.

Quando você cria ou edita um produto, você pode modificar as definições que são usadas para detectar arquivos. As instruções abaixo servem para para editar um produto existente.

Especifique arquivos para detectar a instalação ou uso do produto

1. Clique em **Produtos > Monitorado**s para exibir os produtos monitorados.
2. Clique em um único nome de produto (não um produto normalizado).
3. Clique no botão **Editar** na barra de ferramentas. A caixa de diálogo **Detalhes do produto** é exibida; alguns itens são tipo somente-leitura e outros são editáveis.
4. Em **Status**, selecione **Monitorados** ou **Ignorados** para listar este novo produto em um dos modos de exibição do produto.
5. Clique em **Detecção de instalação**. Todas as opções são somente-leitura.
6. Clique **Detecção de uso**. Você pode adicionar arquivos que indicam o produto está sendo usado.
7. Clique no botão **Adicionar (+)**. Na caixa de diálogo **Adicionar arquivos**, você pode selecionar um nome de arquivo existente (um que existe no banco de dados de inventário), ou você pode clicar em **Definir novo arquivo** e especificar o nome de arquivo, tamanho do arquivo, e número de versão para o arquivo de produto. Repita essas etapas para cada arquivo que quiser usar para determinar quando o produto está em uso. Ao terminar, clique em **OK**.
8. Quando todas as informações estiverem completas, clique em **Salvar**.

Especifique um preço unitário para um produto monitorado

O monitoramento de licenças de softwares inclui vários cálculos diferentes relacionados com o uso de licenças em sua empresa. Por exemplo, o dashboard de Conformidade inclui uma estimativa do custo da conformidade dos produtos instalados com seus termos de licença.

Para cada produto monitorado, você pode especificar o custo unitário que é usado nestes cálculos. O custo que você especifica pode ser diferente que o custo que automaticamente é calculado.

Em situações onde você tem uma licença por um produto, você pode usar o cálculo automático que toma o preço total da licença e o divide pelo número de licenças.

Em situações onde você tem mais de uma licença por um produto, você talvez tenha custos unitários diferentes baseados nos termos da licença. Por exemplo, se você comprou uma licença para uma versão de um produto e comprou uma nova licença para uma mais nova versão, o produto mais novo pode custar mais. Se você pode usar estas licenças para ambas a mais nova versão mais velha do produto, você deverá determinar que preço representa o custo real que você quer usar em cálculos.

Há duas opções para especificar um preço unitário:

- **Usar preço unitário calculado automaticamente em todos os cálculos:** Se você seleciona esta opção, cálculos são baseados nos dados de licença para o produto. Se há uma licença, o preço unitário é calculado dividindo o custo total pelo número de licenças. Se há múltiplas licenças para um produto, o preço unitário é a média do custo unitário de todas as licenças para o produto (todos custos totais divididos pelo número de todas as licenças).
- **Especifique um preço unitário para usar em todos os cálculos:** Se você selecionar esta opção, o preço que você inserir substituirá qualquer cálculo automático para o produto. Por exemplo, se você tivesse várias licenças diferentes para um produto, você poderia especificar o preço atual por licença porque isso é o preço que você pagaria adicionar novas licenças.

Se você encontrar cálculos incorretos no dashboard de SLM, você deve verificar se todas as licenças de um produto têm informações corretas dos custos. Assim, você pode decidir se muda o preço unitário para o produto para representar com exatidão o custo de licenças para o produto.

Para especificar um preço unitário do produto

1. Clique em **Produtos > Monitorado**s para exibir os produtos monitorados.
2. Selecione o produto (usando a caixa de **Pesquisa** desejar encontrar o produto).
3. Clique no botão **Editar** na barra de ferramentas.
4. Clique em **Preço unitário**.
5. Selecione o preço automaticamente calculado, ou clique **Especificar um preço unitário** e entra um custo na caixa de preço unitário.
6. Clique em **Salvar**.

Se você selecionar um produto normalizado, certifique-se que o custo unitário representa todas as versões do produto que são incluídos no produto normalizado.

Use uma consulta para definir quando um produto está instalado

A maioria de produtos são detectados em análises de inventário com arquivos executáveis que indicam um produto foi instalado ou está sendo usado. Em alguns casos você pode detectar que um produto de software está sendo usado em um dispositivo procurando por outros dados do inventário.

Para fazer isto, cria uma consulta na tela de rede do Management Suite que é baseada nos dados do inventário. Você então pode referir-se a consulta como o item usado para detecção de instalação quando você cria um produto personalizado.

Por exemplo, se um produto é licenciado com um dongle que deve ser conectado a um computador para usar o produto, você pode criar uma consulta que identifica o dongle como um item de inventário de hardware. Quando um computador tem o dongle conectado, o analisador de inventário identifica o dongle. Esse dados vinculados ao produto com a ferramenta de monitoramento de licenças de softwares ao associar a consulta ao produto. Em cálculos de SLM, a existência do dongle indica quando o produto está sendo usado.

Outro exemplo é quando você tem uma fonte instalada licenciada por computador. Você pode criar uma consulta com o nome da fonte e versão associe esta a consulta com a definição de produto para a fonte. O analisador de inventário encontrará todos os uso da fonte e que os dados serão relatados ao console do SLM.

IMPORTANTE: Qualquer consulta que você criar para a identificação de produto deve conter Computador.ID como um dos componentes de consulta; se não estiver incluído, não será retornado nenhum dado será retornado da consulta. Adicione o componente a sua consulta e selecione-e como um das colunas exibir.

Para usar uma consulta para detecção de instalação de produto

1. Abra a tela de rede no console do Management Suite e Clique com o botão direito em **Minhas consultas**. Selecionar **Nova consulta**. Defina a consulta com itens que identificam o produto de software que você quer controlar e inclua Computador.ID como um componente. Salve a consulta.
2. Clique em **Ferramentas > Relatórios/Monitoramento > Monitoramento de licenças de softwares** para abrir o console de SLM (Monitoramento de licenças de software).
3. Clique em **Produtos > Monitorado**s. Na barra de ferramentas, clique **Novo > Produto personalizado**.
4. Insira o nome de produto, versão, e nome de fabricante.
5. Clique em **Detecção da instalação** e selecione **Usar detecção de consulta**.
6. Clique em **Procurar**. Em **Minhas consultas**, ache a consulta que você criou. Selecione e clique em **OK**.
7. Adicione dados de qualquer outro produto nas páginas de **Detecção de uso** e de **Preço unitário**. Quando todas as informações estiverem completas, clique em **Salvar**.

Monitoramento de conformidade de licenças de software

A conformidade de licenças de software é uma parte importante do seu gerenciamento de recursos de IT. Você precisa poder mostrar conformidade precisa quando sua organização é auditada e se ela tem diretivas relacionas ao uso de software, a conformidade de licença pode ajudar a seguir as diretivas.

A conformidade da sua organização com os termos de suas licenças de software dependem de:

- Análises precisas do inventário contém dados sobre quais softwares foram descobertos e estão em uso.
- Dados preciso sobre os termos das licenças de software compradas
- Associação correta das licenças com produtos e grupos de computadores
- Reconciliação de dados da licença com dados de inventário

As análises de inventário do LANDesk Management Suite executados nos dispositivos gerenciados da sua rede cuida do primeiro item. Essas análises incluem uma análise do monitoramento de software que salva informações de software no banco de dados.

O segundo item deve ser adicionado ao banco de dados dos registros de licença que sua empresa mantem. Você pode inserir cada licença individualmente ou você pode importar dados de fontes diferentes exportando os dados de uma folha de cálculo do Excel para um arquivo de CSV e então importando os dados no console do SLM.

O terceiro item depende das associações que você faz com produtos quando você adiciona ou edita uma licença. Se você importar dados de licença, verifique cada uma para certificar-se de que ela está associada com produtos cobertos pelos termos da licença. Também, se licenças são limitadas a certos grupos dentro de sua empresa, você deve associar as licenças com os grupos de computador para esses grupos de empresa.

O quarto item é o que a ferramenta de monitoramento de licenças de softwares faz quando todos dados necessários estão disponíveis na banco de dados. A conformidade é calculada todos os dias quando a manutenção do inventário é executada no banco de dados. O êxito do monitoramento de licenças de software depende da precisão dos dados das licenças de softwares e de como as análises de inventário cobrem os dispositivos da empresa. Seus resultados de conformidade também dependem de ter os grupos corretos de computador definiu e associado com licenças.

Tópicos relacionados

"Manter dados precisos das licenças" na página 336

"Criar uma licença" na página 337

"Associar uma licença com produtos" na página 340

Manter dados precisos das licenças

Uma parte importante do gerenciamento financeiro da sua empresa é é a manutenção de licenças de software. A ferramenta de monitoramento de licenças de softwares usa dados da licença para ajudar você a determinar como a sua empresa atende aos termos de suas licenças. Seus dados de licença deve estar disponíveis e exatos para cálculo exato de conformidade.

Você pode querer começar com um número pequeno de licenças, tal como licenças que devem ser controlado para auditorias. Você pode inserir dados da licença manualmente ou importá-los usando o console de monitoração de licença de software. Os dados são usados para gerar estatísticas e relatórios, o que ajuda a determinar se suas licenças de produto estão em conformidade, com base nas instalações reais de produto.

Depois que os dados de licença é adicionado, você deve revisar as informações de produto relacionadas a cada licença. Ache os produtos para uma licença no modo de exibição de produto Descoberto e mova-os para o modo de exibição de Monitorados. Se adequado, combina versões diferentes de um produto em um produto normalizado para que seja mais fácil gerenciar o produtos no console do SLM.

As tarefas a seguir podem ser usadas para manter dados de licenças precisos da sua empresa:

- Criar registros de licença de software
- Importar dados de licença de software
- Criar produtos normalizados
- Associe licenças de software aos produtos instalados

- Exibir a conformidade de licenças de software
- Recalcular a conformidade de licenças de software

Criar uma licença

Se seus dados de licença está num formato não facilmente importado, você pode inserir os dados manualmente no modo de visualização de Licenças. Os dados que você entrar são armazenados no banco de dados e usado par o cálculo.

Para criar um licença

1. Clique em **Produtos > Licenças**.
2. Na barra de ferramentas, clique em **Nova > Licença**.
3. Insira dados nas três páginas da caixa de diálogo do **Criar licença** (Definição, produtos associados e registros).
4. Clique em **Salvar** ao terminar.

Clique aqui para descrições dos campos na caixa de diálogo **Criar licença**.

Página de definições

- **Nome da licença:** O nome da licença, que pode ser o mesmo do produto.
- **Quantidade de licenças:** O número de licenças permitidas no contrato de compra.
- **Preço unitário:** O preço pago pela licença.
- **Grupo de computadores**: Se a licença foi comprada para um grupo específico de computadores, selecione o grupo aqui. Este grupo deve existir no modo de exibição de **Grupos de computadores** do console do SLM e deve ser criado na tela de rede do Management Suite. Selecione **Todos** quando a licença puder ser usada para qualquer computador na sua organização. Se o grupo que você quer não está listado, clique em **Criar grupo de computadores** para criar um novo grupo de uma consulta ou grupo de dispositivos do Management Suite.
- **Fornecedor:** O fornecedor de quem você adquiriu a licença. Esse pode ser o mesmo do fabricante. Depois de digitar pelo menos três caracteres, todos os nomes correspondentes de fornecedores no banco de dados são exibidos; selecione o correspondente da lista.
- **Data da compra:** A data em que a licença foi adquirida e a validade. Clique no ícone do calendário para selecionar a data ou o tipo de data na caixa de texto (ela será apresentada no seu formato numérico, como dd/mm/aaaa).
- **Data de vencimento**: A data em que a licença vence. Esta data é importante quando você deseja fazer controle de licenças que precisam ser renovadas. Clique no ícone do calendário para selecionar a data ou o tipo de data na caixa de texto (ela será apresentada no seu formato numérico, como dd/mm/aaaa).
- **Consumo**: O método usado para calcular o uso da licença.
    - **Um por computador**: O uso da licença é contado uma vez para cada computador que tem o software instalado, independentemente de quantas instalações possa haver no computador.
- **Tipo de conformidade**: O tipo de licença, em termos de conformidade de licença como especificado pelo fabricante.
    - **Calculado**: O uso da licença é calculado para garantir que está em conformidade com os termos da venda. Isto pode incluir os seguintes tipos de licença: Novo produto, Atualização competitiva, Licença de OEM, Atualização de produto, Licença em lote, Contrato de empresa

ou Desconhecido.

- **Não calculado**: O uso da licença não precisa ser calculado para estar em conformidade. Isto pode incluir os seguintes tipos de licença: Software gratuito, Domínio público, Shareware, Licença flutuante e licença de local.

Página de produtos associados

Esta página lista os produtos associados a licença. Liste todos os produtos que podem ser usados sob os termos da licença.

Liste os produtos na ordem que você quer que consumam as licenças. O primeiro produto consume primeiro as licenças disponíveis. Se existem licenças adicionais disponíveis, então o segundo produto consume licenças disponíveis. Isto continua abaixo a lista até que nenhumas mais licenças estão disponíveis.

Você pode associar qualquer produto com uma licença. Se o produto atualmente não é monitorado, o SLM moverá o produto para a lista de Monitorados quando você o associar a uma licença.

Para adicionar produtos associados à lista

1. Clique no botão **Adicionar (+)**.
2. Na caixa de diálogo **Adicionar produtos à licença**, digite ao menos três caracteres no campo **Nome do produto contém** para achar os produtos que você quer. Todos os produtos correspondentes ao string que você digitar são listados nos resultados.
3. Para filtrar a lista de resultados, você pode digitar uma string na caixa **Nome do produto não contém**. Produtos com este string serão removidos da lista. Você pode usar string múltiplos, separados por espaço.
4. Para limitar os resultados a produtos no modo de exibição **Controlada** de produto, selecione **Exibir somente produtos monitorados**.
5. Selecione um ou mais produtos da lista de resultados e clique em OK.

   Os produtos são adicionados a lista **Produtos associados**.
6. Use as setas para cima e abaixo para mover produtos para cima ou para baixo na lista.

Tópicos relacionados

"Associar uma licença com produtos" na página 340

Páginas de registro

Esta página contém dados e anotações que documentam a licença em termos de seu compra ou contabilidade da empresa pratica. Essas informações não são usadas no monitoramento de licença mas são uteis para manter registros exatos em caso de auditoria.

- **Número de fatura do fabricante:** O número da fatura emitido pelo fabricante do software. Isto é útil para controle do software dentro do seu processo de compra.
- **Número da ordem de compra:** O número de pedido de compra da sua organização usado para comprar o software. Isto é útil para controle do software dentro do seu processo de compra.
- **Código da licença**: O código fornecido pelo fabricante para ativar a licença.
- **Número de série**: O número de série do fabricante associado à licença.
- **Local**: Uma anotação que ajuda a identificar onde as licenças estão sendo usadas na sua organização.

- **Documentos de apoio:** Uma observação que descreve onde a documentação de apoio das suas licenças pode ser encontrada. Isto pode indicar um local na rede ou URL ou qualquer descrição que você quiser usar.
- **Notas:** Digite qualquer nota adicional para a licença. Essas notas são salvas no banco de dados.

Importar dados da licença de um arquivo CSV

Você pode importar dados da licença de uma versão anterior do LANDesk Management Suite ou de outra fonte de dados. Os dados devem ser salvos como um arquivo de CSV.

Um arquivo de amostra CSV (ImportLicense.csv) está incluído no compartilhamento LDMAIN do servidor núcleo (na pasta LDMAIN\LANDesk\SAM), para consulta As seguintes orientações para criar um arquivo de CVS para importar dados de licença:

- A única coluna necessária no arquivo de CSV é a coluna de Nome
- Se você não sabe o que colocar em uma coluna, deixe-o espaço em branco. O processo de importação adicionará um valor padrão para qualquer coluna em branco.
- Depois das colunas de propriedade de licença, há colunas para produtos associados. Eles são chamados "Produto associado 1" e "Versão 1 do produto", "Produto associado 2" e "Versão 2 do produto" e assim por diante. Ponha o nome de produto na coluna "Produto associado x" e a versão do produto na coluna "Versão x do produto" Se não há nenhuma versão de produto, deixe o espaço em branco de coluna. O processo de importação procurará produtos combinados com o nome fornecido de produto e versão. Se múltiplos produtos são encontrados com o mesmo nome e versão, todos os produtos combinados serão associados com a licença. Qualquer número de produtos pode ser associado a uma licença.
- A *importação não anulará* licenças existentes. Se uma licença existente combina o nome de uma licença sendo importada, será criada uma nova licença com o nome de "<License name> [1]". O número entre chaves será aumentado com cada correspondência, assim cada licença terá um nome exclusivo.

Para importar dados de licença

1. Prepare um arquivo de CSV com os dados de licença que você quer importar, usando as orientações listadas acima.
2. No console do SLM, clique em **Produtos > Licenças**. Na barra de ferramentas, clique em **Ações > Importação de CSV**.
3. Navegue ao local do seu arquivo CSV clique em **Abrir**.

   Os dados da licença são adicionados ao banco de dados e exibidos no modo de exibição de **Licenças** do console do SLM.

4. Para revisar as licenças importadas e editar os dados, selecione uma licença na tela de **Licenças** e no botão **Editar** botão. Revise os dados em cada um das três páginas do diálogo (Definição, Produtos associados, e Registros). Clique em **Salvar** ao terminar.

Associar uma licença com produtos

Quando você adiciona ou edita uma licença, você deve associar-se a licença com um ou mais produtos para calcular conformidade para uso de produto e a licença. Você pode selecionar um ou mais produtos, inclusive produtos normalizados que representam múltiplos produtos individuais. Se um produto atualmente não é monitorado, o SLM moverá o produto para lista de Monitorados quando você o associa-se com uma licença.

Quando você seleciona produtos associados, lista os produtos na ordem que você quer que os consumam as licenças. O primeiro produto consume primeiro as licenças disponíveis. Se existem licenças adicionais disponíveis, então o segundo produto consume licenças disponíveis. Isto continua abaixo a lista até que nenhumas mais licenças estão disponíveis.

A seguir um exemplo de como o cálculo de licença é aplicado com múltiplas versões de produto:

- Você comprou uma licença para Produto ABC que permite 30 instalações (ou estações de licença)
- A licença pode ser usada para versões 3, 4, e 5 desse produto
- Na lista de **Produtos associados**, você ordenou por versões mais recentes, (5) primeiro seguida por versão 4 e a versão 3

Nesta situação, o uso de licença é calculado como segue:

- 16 usuários têm versão a 5 instalada, portanto todos os 16 usarão uma licença
- 21 usuários têm versão 4 instalada; 14 deles usam uma estação de licença e 7 não licenciados
- 8 usuários têm a versão 3 instalada; nenhum deles são licenciados

Seus relatórios de conformidade de licença para este produto mostrarão que 15 usos do produto não são cobertos pela licença. Você então deve determinar se comprar licenças adicionais. Você também talvez revise o uso real dos produtos em sua empresa. Se alguns usuários com o produto não instalaram usaram o produto por um período longo de tempo, você pode verificar com eles ver se eles necessitam o software. Se não, eles podem desinstalar o produto e suas licenças pode ser aplicado a outros usuários.

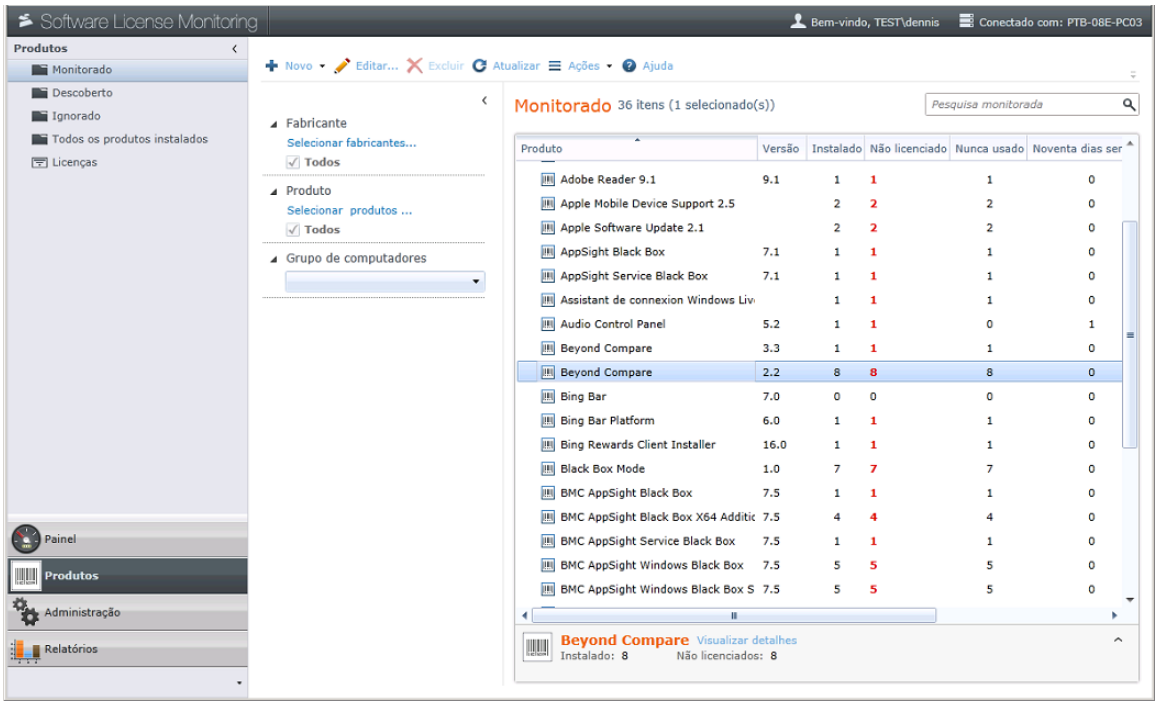
NOTA: As licenças são associadas com produtos para cálculo de conformidade. Se você apagar um produto, a licença associada com aquele produto não será mais associada com ele, e relatórios de conformidade não irão mais exibir aquele produto como licença de consumo.

Exibição dos dados de conformidade da licença

No console do SLM, há maneiras diferentes descobrir se suas instalações de produto estão em conformidade com os termos de suas licenças de software. Este tópico descreve como achar os dados que você necessita.

Ver informações por produto

Abra o modo de exibição de produto **Monitorados** para ver informações sobre os produtos instaladas em sua empresa. Um produto deve ser movido ao modo de de exibição Monitorado para que você encontre o máximo de informações sobre seu uso e licença.


Software License Monitoring
Bem-vindo, TEST\dennis
Conectado com: PTB-08E-PC03
Produtos
Monitorado
Descoberto
Ignorado
Todos os produtos instalados
Licenças
Novo
Editar...
Excluir
Atualizar
Ações
Ajuda
Fabricante
Selecionar fabricantes...
Todos
Produto
Selecionar produtos ...
Todos
Grupo de computadores
Monitorado 36 itens (1 selecionado(s))
Pesquisa monitorada
Produto
Versão
Instalado
Não licenciado
Nunca usado
Noventa dias ser
Adobe Reader 9.1 9.1 1 1 1 0
Apple Mobile Device Support 2.5 2 2 2 0
Apple Software Update 2.1 2 2 2 0
AppSight Black Box 7.1 1 1 1 0
AppSight Service Black Box 7.1 1 1 1 0
Assistant de connexion Windows Liv 1 1 1 0
Audio Control Panel 5.2 1 1 0 1
Beyond Compare 3.3 1 1 1 0
Beyond Compare 2.2 8 8 8 0
Bing Bar 7.0 0 0 0 0
Bing Bar Platform 6.0 1 1 1 0
Bing Rewards Client Installer 16.0 1 1 1 0
Black Box Mode 1.0 7 7 7 0
BMC AppSight Black Box 7.5 1 1 1 0
BMC AppSight Black Box X64 Additic 7.5 4 4 4 0
BMC AppSight Service Black Box 7.5 1 1 1 0
BMC AppSight Windows Black Box 7.5 5 5 5 0
BMC AppSight Windows Black Box S 7.5 5 5 5 0
Beyond Compare Visualizar detalhes
Instalado: 8 Não licenciados: 8
Painel
Produtos
Administração
Relatórios

É possível especificar os seguintes itens:

- **Instalações do produto**: Clique duas vezes no nome do produto para ver uma lista de dispositivos com o produto instalado.
- **Se está em uso atualmente**: Veja as colunas **Nunca usados** e **Noventa dias sem uso** no modo de exibição Monitorados para ver se há usuários que não estão usando o produto ou que o usam esporadicamente.
- **Se estiver adequadamente licenciado**: Compare as colunas **Instaladas** e **Sem licença** no modo de exibição Monitorados para ver se há mais cópias instaladas do que licenças válidas.
- **Licenças associadas ao produto:** Clique com o botão direito em um produto e selecione **Exibir licenças que coincidem com o produto selecionado** para ver uma lista das licenças associadas ao produto.

NOTA: Você notará que os modos de exibição **Descobertos** e **Ignorados** têm as mesmas colunas e parecem exibir dados de conformidade, os dados não com representam as licenças comparadas com instalações reais de produto com exatidão. Só os produtos no modo de exibição de produtos **Monitorados** que estiverem associados a licenças exibirão dados úteis e precisos.

Exibindo dados de resumo de conformidade

Os dashboards de instrumentos contêm dados de resumo relacionou autorizar conformidade e otimização. Estas páginas são projetadas ajudar você age nos problemas mais importantes relacionados a software autorizando. Eles não fornecem uma visão geral, mas vão lhe guiar para encontrar os problemas que devem ser resolvidos primeiro para que você pode reduzir custos e melhorar eficiência do uso de softwares.

- **Dashboard de auditorias:** Esta página inclui relatórios que são útil quando você prepara para uma auditoria de seu uso de licença de software.

- **Dashboard de conformidade**: Esta página inclui relatórios que mostram você produtos que são para fora de conformidade com termos de licença e necessita sua atenção.
- **Dashboard de otimização de licenças**: Esta página inclui relatórios que calculam a economia que você pode fazer removendo softwares não usados de computadores em sua empresa.

Exibição de relatórios relacionados a licenças

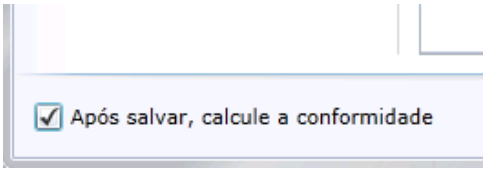
Os relatórios de SLM trazem juntos completam dados reportagem para muitos aspectos de sua conformidade de licença de software e uso. Use relatórios para encontrar todos os detalhes para um problema ou necessidade específica e exportar os dados ou e-mail o relatório para outros para agirem.

- **Relatórios de auditoria**: Estes relatórios são úteis quando você prepara para uma auditoria do seu uso de licença de software. Eles incluem sinalizadores de auditoria como produtos monitorados sem licenças associadas e licenças que não têm dados de suporte, como número de fatura ou da ordem de compra.
- **Relatórios de conformidade**: Estes relatórios incluem detalhes para todos os produtos e licenças que são para fora de conformidade. Eles incluem uma modo de exibição geral de consumo de licença para todos os produtos, custos de total trazer produtos em conformidade, e assim por diante.
- **Relatórios de otimização de licenças**: Estes relatórios fornecem detalhes que podem ajudar você otimiza seu uso da empresa de software. Eles incluem listas de licenças não utilizadas de software, produtos não usaram nem raramente usado, e outros dados relacionados.

Recalcular conformidade de licença

A conformidade da licença é calculada diariamente durante a execução da manutenção do inventário no banco de dados.

Em muitas tarefas relacionadas a produtos e licenças, um novo cálculo é executado quando você grava os dados alterados. Ao encontrar uma caixa de seleção chamada **Calcular conformidade após salvar**, significa que ao salvar seu trabalho o cálculo de conformidade de licença será executado outra vez.

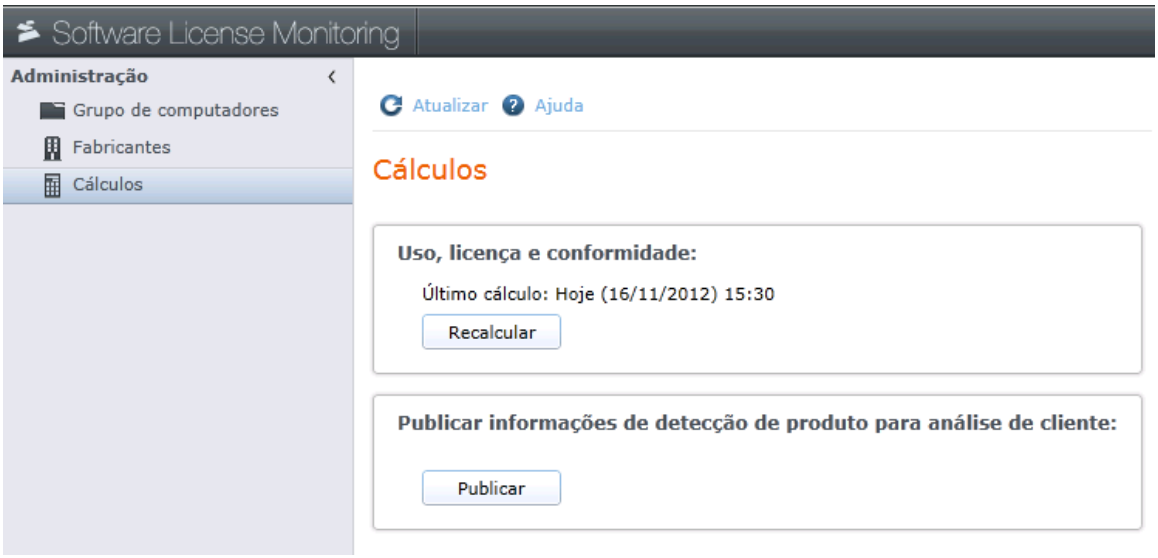


Se você adicionou dados de licença ou fez outras mudanças e quer recalcular a conformidade sem esperar a manutenção agendada, você pode iniciar um novo cálculo de uso de produto e conformidade de licença.

Uma opção relacionada permite que você adicione novas informações de detecção de produto ao arquivo de análise de inventário que é usado para detectar quando produtos são instalados ou usados. Se você definiu instalação de produto ou uso especificando os arquivos que identificam um produto, você pode publicar esta informações para que fique disponível na próxima vez que a análise de inventário em dispositivos gerenciados seja executada.

Recalcular uso e conformidade

1. Clique em **Administração > Cálculos**.



2. Para atualizar uso e conformidade de licença, clique em **Recalcular**.
3. Para publicar novas informações de detecção de produto que usadas em análises de inventário de cliente, clica em **Publicar**.

Crie um relatório com dados do monitoramento da licença de software

A ferramenta de reportagem LANDesk Management Suite está disponível para uso com o console de monitoramento de licença de software. Use-o para criar um relatório próprio para imprimir dos dados atualmente exibiu no console.

Quando você cria um relatório da modo de exibição atual, o relatório contém todos itens atualmente listados. Os dados são organizado com as mesmas colunas que são exibidas no modo de exibição atual. Você pode salvar o relatório em seis formatos diferentes.

Você também pode executar relatórios de predefinido que são fornecidos com a característica de reportagem. Esses relatórios estão relacionados na página **Relatórios** do console do SLM.

IMPORTANTE: Se você usar o Internet Explorer 9 para o console do SLM, você deve ativar o modo de visualização de Compatibilidade para ver os relatórios Management Suite. Para ativar o modo de visualização de Compatibilidade, inicie o Internet Explorer 9. Pressione a tecla **Alt** para ver o menu e clique em **Ferramentas > Configurações da tela de compatibilidade**. Selecione a **Exibir todos os sites no modo de visualização de Compatibilidade** e clique em **Fechar**.

Para criar um relatório de dados no console

1. Veja todos os dados da licença ou do produto no console do SLM.
2. Na barra de ferramentas, clique **Ações > Relatório para impressão dos resultados da pesquisa**.

   O relatório abre numa janela separada de exibição de relatórios.
3. Na barra de ferramentas do visualizador de relatório, selecione um formato de relatório.

4. Para salvar uma cópia do relatório, clique o botão **Exportar** na barra de ferramentas.
5. Clique em **Navegar** e selecione um local para salvar o arquivo. Clique em **Salvar** e clique em **Exportar** para salvar o relatório.

Em algumas páginas há um botão de relatório que você pode clicar no lugar de usar a barra de ferramentas no passo 2.

Para executar um relatório de predefinido

1. No console do SLM, clique em **Relatórios**.
2. Clique em **Relatórios > Relatórios padrão > Monitoramento de licenças de softwares** e localize o relatório desejado.
3. Selecione o relatório e clique em **Executar relatório** na barra de ferramentas.

   O relatório abre numa janela separada de exibição de relatórios.
4. Na barra de ferramentas do visualizador de relatório, selecione um formato de relatório.
5. Para salvar uma cópia do relatório, clique o botão **Exportar** na barra de ferramentas.
6. Clique em **Navegar** e selecione um local para salvar o arquivo. Clique em **Salvar** e clique em **Exportar** para salvar o relatório.

Definir um grupo de computadores

Como você controla software e uso de licença, você pode querer associar os grupos de computadores com licenças. Por exemplo, um grupo pode representar computadores em um local ou e, uma divisão de sua empresa com sua própria contabilidade de licenças de softwares.

Você pode associar licenças com os grupos em duas maneiras:

- **Grupo estático**: um grupo de computadores que você selecionou na tela de rede do Management Suite e salvo como um grupo de dispositivo.
- **Grupo dinâmico**: um grupo de computadores definidos com uma consulta no modo de exibição de rede do Management Suite. Como dispositivos controlados são adicionados ou removidos, o conteúdo do grupo muda para corresponder aos parâmetros da consulta.

Você só pode criar os grupos na Management Suite modo de exibição de rede. Ao definir um grupo no console do SLM, você está simplesmente escolhendo um nome para associar com um grupo existente de dispositivos ou consulta.

Para definir um grupo de computadores

1. Clique em **Administração > Grupos de computadores**.
2. Na barra de ferramentas, clique **Novo > Grupo de computadores**.
3. Digite um nome para o grupo. Este nome identifica o grupo no console do SLM.
4. Expanda **Dispositivos** ou **Consultas** e ache o grupo de dispositivos ou consulta que é a fonte para o grupo de computadores.
5. Quando todas as informações estiverem completas, clique em **Salvar**.

Para excluir um grupo de computadores

1. Clique em **Administração > Grupos de computadores**.
2. Selecione um grupo na lista. Na barra de ferramentas, clique no botão **Excluir**.
3. Clique **Sim** confirmar a anulação.

NOTA: Se excluir um grupo de computadores, todas as licenças associadas não serão mais associadas com esses computadores, assim os relatórios de conformidade não se aplicarão ao grupo. Se você faz isto, você deve decidir que computadores associar com a licença e define outro grupo. Se não há nenhum grupo associado, a licença é associada com todos os computadores.

Exibir produtos instalados para um grupo de computadores

Inicialmente, todos produtos descobertos em todos os computadores em seu banco de dados de inventário são encontrados no modo de exibição de produto **Descoberto**. Isso pode ser adicionado rapidamente a um grande número de registros. Mova produtos para os modos de exibição de produtos **Monitorados** ou **Ignorados** para identificar os produtos que você quer controlar ativamente e para aqueles que você não se interessa em monitorar.

Como você define os grupos de computadores, exibir somente o software instalado em um grupo de computadores. Isso é uma maneira útil ver um grupo menor de registros de produtos para computadores selecionados.

Para exibir produtos instalados para um grupo de computador

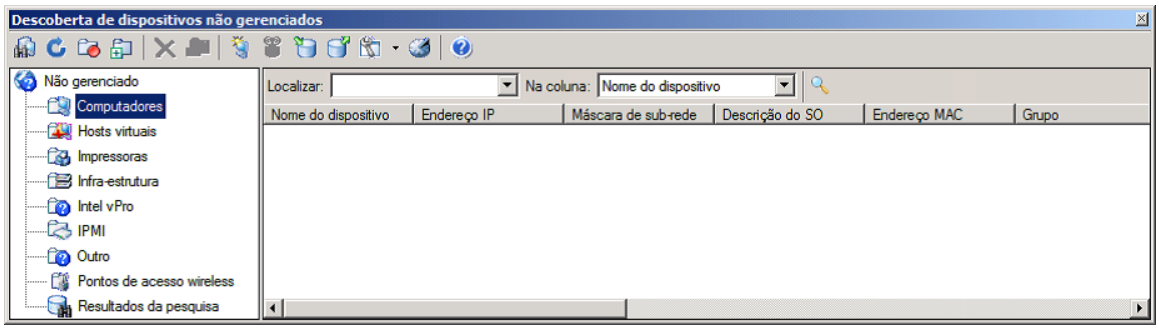
1. Clique **Produtos** e selecione **Monitorado**, **Descoberto**, **Ignorado**, ou **Todos os produtos instalados**.
2. Em **Grupo de computadores**, selecione um grupo de computadores da lista.

A lista muda para exibir somente os produtos instalados nos computadores no grupo que você selecionou.

Descoberta de dispositivos não gerenciados

Visão geral da descoberta de dispositivos não gerenciados

A descoberta de dispositivos não gerenciados (UDD) fornece várias maneiras para analisar e detectar dispositivos não gerenciados na rede.



Métodos de análise básicos da UDD:

- **Análise de rede:** Procura computadores fazendo uma varredura de ping ICMP. Essa é a pesquisa mais completa, porém a mais lenta. Você pode limitar a pesquisa a determinadas faixas de IP e sub-redes. Como padrão, essa opção usa o NetBIOS para tentar coletar informações sobre o dispositivo.
  - **Impressão digital de SO de IP:** Use nmap para tentar descobrir mais sobre um dispositivo, como que sistema operacional está sendo executado.
  - **SNMP:** UDD usa SNMP para descobrir dispositivos. Clique em **Configurar** para digitar informações sobre o seu SNMP na sua rede.
- **Agente padrão do LANDesk:** Procura pelo agente LANDesk padrão (CBA) nos computadores. Esta opção descobre computadores que têm os produtos LANDesk instalados.
- **Domínio de NT:** Procura dispositivos em um domínio especificado. Descobre membros, estando o computador ligado ou desligado.
- **LDAP:** Procura dispositivos em um diretório especificado. Descobre membros, estando o computador ligado ou desligado.
- **IPMI:** Procura os servidores habilitados com o IPMI - Intelligent Platform Management Interface, o que permite que você acesse muitos dos recursos do servidor, independentemente de o servidor estar ligado ou desligado ou do estado no qual o SO se encontra.
- **Hosts virtuais:** procura servidores executando VMware ESX Server. Esses servidores aparecem na pasta **Hosts virtual**.

Para automatizar a descoberta de dispositivos não gerenciados, você pode agendar a análise UDD para que ocorra periodicamente. Por exemplo, você poderia dividir sua rede em três partes e agendar uma varredura de ping para um terço a cada noite.

Se você agendar uma descoberta, o servidor núcleo fará a descoberta. Descobertas não agendadas ocorrem a partir do console que as inicia.

Descoberta de dispositivos estendida

A ferramenta UDD também suporta a análise de descoberta de dispositivos estendida (XDD). A XDD depende de um agente de dispositivo (distribuído através de uma configuração de agentes) para escutar difusões ARP e sinais WAP na rede LANDesk. O agente XDD em um dispositivo configurado e verifica se o dispositivo de multidifusão tem o agente LANDesk padrão instalado. Se o agente LANDesk padrão não responder, um dispositivo descoberto ARP é exibido no grupo **Computadores** com informação relatada na tela de listagem do item e um dispositivo WAP é exibido no grupo **Pontos de acesso wireless** com a informação relatada na tela de listagem.

A descoberta estendida de dispositivo é ideal nas situações que envolvem firewalls as quais impedem os dispositivos de responderem aos métodos de descoberta UDD baseada em ping.

NOTA: Usar a descoberta estendida de dispositivos para descobrir dispositivos com firewall ativado
Lembre-se que normalmente os métodos normais de descoberta de dispositivos não gerenciados não podem descobrir dispositivos que usam firewall como, por exemplo, o Windows Firewall integrado ao Windows. Tipicamente, a firewall impede o dispositivo de responder aos métodos de descoberta que a descoberta de dispositivos não gerenciados utiliza. A descoberta estendida de dispositivo ajuda a resolver este problema usando o tráfego ARP de rede para descobrir dispositivos.

Tópicos relacionados

"Distribuição de agentes LANDesk para dispositivos não gerenciados" na página 347

"Descoberta de dispositivos não gerenciados com UDD" na página 348

"Trabalhar com dispositivos encontrados com XDD" na página 355

"O que acontece quando um dispositivo é descoberto" na página 354

"Uso da descoberta estendida de dispositivos (ARP e WAP)" na página 351

"Ajuda da descoberta de dispositivos não gerenciados" na página 357

Distribuição de agentes LANDesk para dispositivos não gerenciados

Após ter descoberto dispositivos não gerenciados usando os métodos de análise e descoberta descritos acima, você pode distribuir agentes LANDesk para esses dispositivos usando um dos seguintes métodos:

- Distribuições com base na instalação por envio usando tarefas agendadas e uma conta administrativa de domínio que você configurou para o Agendador.
- Distribuições baseadas em envio usando o agente LANDesk padrão. Se os dispositivos têm o agente LANDesk padrão, você pode fazer uma distribuição baseada em envio.
- Distribuição com base na instalação por envio usando um script de logon.

Mais informações sobre a distribuição de dispositivos estão disponíveis na comunidade LANDesk http://community.landesk.com.

Ao organizar dispositivos para a distribuição de agentes, pode ser mais fácil ordenar a lista de dispositivos não gerenciados pelo agente LANDesk padrão para agrupar por distribuições de dispositivos agente LANDesk padrão e ordenar por domínio para distribuições por tarefas agendadas.

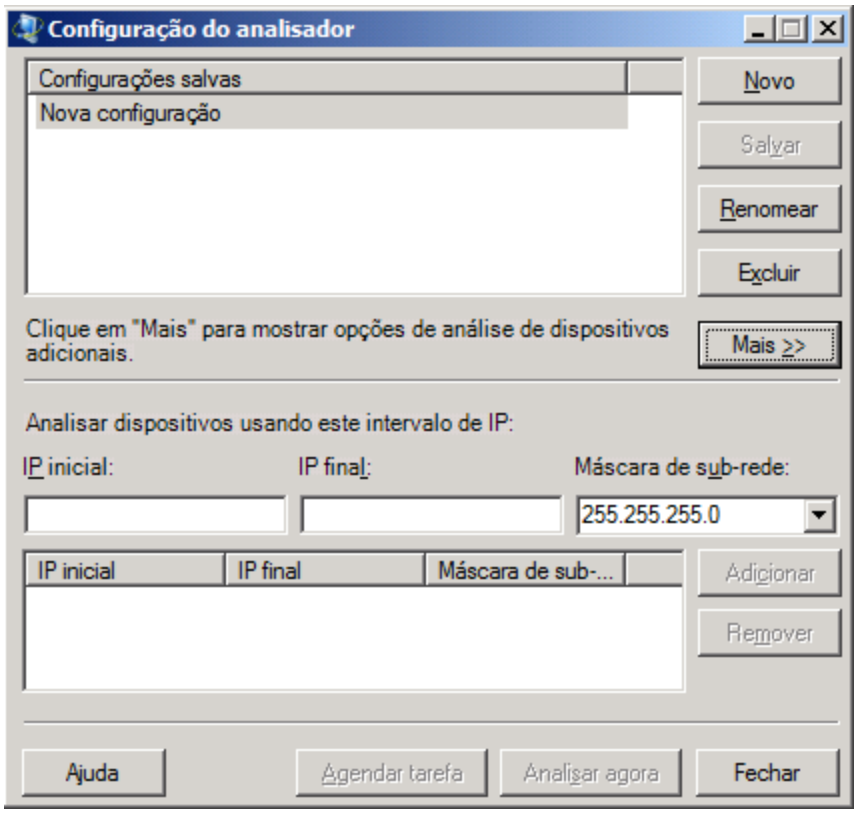
NOTA: Distribuição para dispositivos Windows XP
A configuração pré-definida do Windows obriga logons de rede que utilizam uma conta local para iniciar a sessão utilizando, em vez disso, a conta de convidado. Se você não estiver usando uma conta administrativa de nível de domínio, e estiver usando uma conta local para o serviço Agendador, as tarefas agendadas não serão executadas porque o serviço Agendador não poderá efetuar a autenticação.

Para distribuir agentes LANDesk a dispositivos não gerenciados

1. Clique em **Ferramentas > Configuração > Configuração do agente** e crie uma nova configuração ou use uma já existente. No menu de atalho dessa configuração, clique em **Agendar**.
2. Clique em **Ferramentas > Configuração > Descoberta de dispositivos não gerenciados** e selecione os dispositivos que deseja distribuir. Arraste os dispositivos para a janela **Tarefas agendadas**. Se a janela **Tarefas agendadas** estiver minimizada, você poderá arrastar dispositivos para a guia **Tarefas agendadas**. Isto abrirá a janela **Tarefas agendadas**.
3. Caso os dispositivos não tenham o agente LANDesk padrão, clique em **Configurar > Serviços** e clique na guia **Agendador**. Certifique-se de que a conta Agendador tenha privilégios administrativos nos dispositivos para os quais você está distribuindo.
4. Clique duas vezes no script de distribuição e defina uma hora de início. Clique em **OK** quando tiver concluído.
5. Observe as atualizações na janela **Tarefas agendadas**.

Descoberta de dispositivos não gerenciados com UDD

É fácil descobrir dispositivos não gerenciados como os métodos básicos de análise de UDD.



Para descobrir dispositivos não gerenciados com UDD

1. Na janela Descoberta de dispositivos não gerenciados (**Ferramentas > Configuração > Descoberta de dispositivos não gerenciados**), clique no botão **Varredura de rede**.
2. Clique em **Mais >>** selecione as opções de descoberta desejada. O tipo de descoberta padrão usa uma análise de rede padrão com impressão digital IP SO dos dispositivos descobertos.
3. Informe um intervalo inicial e final de IP para a varredura. Você deve inserir um intervalo de **Descoberta do agente LANDesk padrão** (CBA) ou **Descoberta de rede** para que funcione. O intervalo é opcional para **Domínios NT** e **LDAP**.
4. Informe uma **Máscara de sub-rede**.
5. Clique no botão **Adicionar** para incluir a varredura que você acabou de configurar na lista de tarefas.
6. Na lista de tarefas na parte inferior da caixa de diálogo, selecione as varreduras que você deseja executar e clique no botão **Varrer agora** para efetuar a varredura imediatamente, ou no botão **Agendar tarefa** para executar as varreduras posteriormente ou em um agendamento recorrente. Os botões **Varrer agora** e **Agendar tarefa** executam apenas as varreduras que você incluiu na lista de tarefas e que estiverem selecionadas.
7. Observe a caixa de diálogo Status da varredura para ver se esse status é atualizado. Quando a análise terminar, clique em **Fechar** nas caixas de diálogo Status da análise e Configuração do analisador.
8. Clique em **Computadores** da árvore UDD para ver os resultados da varredura.

Configuração do descoberta de domínios do Windows NT

A opção de descoberta de domínios do Windows NT não funcionará se você não configurar o serviço Agendador para iniciar sessão no domínio com uma conta de administrador do domínio.

Para configurar a conta de logon do Planejador

1. Clique em **Configurar > Serviços** e clique na guia **Planejador**.
2. Clique em **Alterar login**.
3. Digite um nome de usuário e uma senha válidos para o administrador de domínio.
4. Clique em **OK**.
5. Reinicie o serviço Agendador para que a alteração seja aplicada. Na guia **Planejador**, clique em **Parar** e, quando o serviço for interrompido, clique em **Iniciar**.

Manutenção de registros do dispositivo ARP descoberto

O UDD armazena dispositivos encontrados através da descoberta estendida de dispositivo no banco de dados do servidor núcleo. Se tiver muitos dispositivos não gerenciados na sua rede, esses dados podem acumular muito rapidamente. Como padrão, esses dados são mantidos por 24 horas. Você pode personalizar o tempo que os dispositivos encontrados pela descoberta estendida de dispositivo ficam no banco de dados. Após o número de dias especificados, os dispositivos que não forem redescobertos dentro do período serão apagados.

Para configurar o histórico de descoberta ARP

1. Clique em **Ferramentas > Configuração > Descoberta de dispositivo não gerenciado**.
2. Clique no botão da barra de ferramentas **Configurar histórico de descoberta ARP**.
3. Mude as opções desejadas. Clique em **Ajuda** para ver mais informações.
4. Clique em **OK** ao terminar.

Restaurar os registros do cliente

Se o banco de dados núcleo for, por acaso, reconfigurado e precisar restaurar os dados dos dispositivos, você pode usar a UDD para descobrir todos os dispositivos na rede. Você pode usar os resultados de descoberta como o alvo para a tarefa agendada "Restaurar registros do cliente".

Se os dispositivos tiverem o agente LANDesk padrão, essa tarefa fará os dispositivos enviarem uma análise completa de inventário para o banco de dados núcleo para o qual cada dispositivo está configurado localmente. Como resultado dessa tarefa, os dispositivos que já tiverem sido configurados serão reanalisados e recolocados no banco de dados e os dispositivos continuarão apontando para o servidor núcleo de gerenciamento correto. A tarefa falhará nos dispositivos que não tiverem sido gerenciados por um servidor núcleo.

Para restaurar os registros do cliente

1. Use UDD para descobrir dispositivos não gerenciados, conforme descrito anteriormente.
2. Clique em **Ferramentas > Distribuição > Tarefas agendadas**.
3. No painel **Tarefas agendadas**, clique no botão **Agendar script**.
4. Clique em **Restaurar registros do cliente** e no respectivo menu de atalho, clique em **Agendar**.
5. Na árvore **Localizar resultados** UDD, arraste os computadores que quiser restaurar na tarefa **Restaurar registros do cliente** na janela **Tarefas agendadas**.
6. No menu de atalho da tarefa **Restaurar registros do cliente**, clique em **Propriedades** e termine a configuração da tarefa.
7. Observe as atualizações na janela **Tarefas agendadas**.

Entendendo a filtragem de Endereço IP com o Descoberta estendida de dispositivo (XDD)

Não recomendamos a instalação da descoberta de dispositivos estendidos em computadores notebook. Eles podem estar conectados a outras redes que você não deseja monitorar, como, por exemplo, redes de hotéis ou aeroportos. Para impedir a descoberta de dispositivos que não estejam em sua rede, o servidor núcleo ignora endereços IP onde o primeiro e segundo octetos são 10 números maiores ou menores do que o do servidor núcleo. Por exemplo, se o endereço IP do seu servidor núcleo for 192.168.20.17, a descoberta do dispositivo estendido no servidor núcleo irá ignorar os endereços acima de 203.179.0.0 e abaixo de 181.157.0.0.

Para desativar esse recurso, acrescente a seguinte chave de registro DWORD ao servidor núcleo e configure o seu valor em 0:

- HKEY_LOCAL_MACHINE\SOFTWARE\LANDesk\ManagementSuite\XDD\Filter

Para reativar o filtro, configure o valor em 1.

Para ajustar as faixas de monitoramento do primeiro e segundo octetos, adicione as seguintes chaves de registro DWORD ao servidor núcleo e configure seus valores à faixa numérica que quiser monitorar (o padrão é 10 para o primeiro e segundo octetos):

- HKEY_LOCAL_MACHINE\SOFTWARE\LANDesk\ManagementSuite\XDD\FilterThreshold1
- HKEY_LOCAL_MACHINE\SOFTWARE\LANDesk\ManagementSuite\XDD\FilterThreshold2

FilterThreshold1 contém a faixa para o primeiro octeto e FilterThreshold2 contém a faixa para o segundo octeto.

Uso da descoberta estendida de dispositivos (ARP e WAP)

A Descoberta estendida de dispositivos (XDD) funciona fora dos métodos de descoberta baseados em análise, geralmente usados pela UDD. O agente XDD pode ser configurado e distribuído para gerenciar dispositivos a usarem os métodos de descoberta ARP e/ou WAP. Esta seção descreve os dois métodos de descoberta.

Método de descoberta ARP

Os dispositivos gerenciados configurados com o agente de XDD estão alertas para difusões ARP (Protocolo de resolução de endereço) e mantêm um cache (na memória e em um arquivo na unidade local) dos dispositivos que as fazem. Os dispositivos em rede usam ARP para associar um endereço TCP/IP com um endereço MAC de hardware da rede do dispositivo. Essa comunicação ocorre em um nível muito baixo e não depende de dispositivos que respondem a pings ou de comunicação de agente em portas específicas de rede. Mesmo os dispositivos com firewall muito fortes dependem do ARP. Por esse motivo, a descoberta de dispositivos estendida pode ajudar a encontrar dispositivos que as análises de descoberta normais não descobrem.

Quando uma nova difusão de ARP é reconhecida por um dispositivo configurado com o agente de descoberta de dispositivos estendida, os agentes que detectam o ARP aguardam dois minutos para detectar o dispositivo para reinicializar e, a seguir, cada agente aguarda por um tempo aleatório. O agente com a espera aleatória mais curta fará o ping para o novo dispositivo primeiro, verificando a existência de agentes LANDesk e, a seguir, o UDP faz a difusão para a sub-rede para informar os outros agentes que cuidou do ping para aquele dispositivo. Se você tiver vários agentes de descoberta estendida de dispositivo instalados, isso impede os dispositivos de gerarem tráfego em excesso se todos fizerem ping ao mesmo tempo.

Como padrão, o tempo limite das tabelas de ARP armazenadas pelo agente de descoberta estendida de dispositivo vence após 48 horas. Isso significa que será feito ping para cada dispositivo de rede uma vez durante o tempo limite. Só é feito um ping por tempo limite mesmo para os dispositivos que geram grande quantidade de tráfego ARP.

Assume-se que os dispositivos com agentes LANDesk sejam gerenciados e não são reportados ao servidor núcleo. Os dispositivos sem agentes LANDesk são reportados ao servidor núcleo como dispositivos não gerenciados. Esses dispositivos aparecem na lista **Computadores** da janela **Descoberta de dispositivo não gerenciado**. Os dispositivos descobertos através de ARP mostram **Verdadeiro** na coluna **Descoberto por ARP**. Para dispositivos ARP não gerenciados descobertos, XDD reporta a seguinte informação nas colunas de visualização de listagem:

- Endereço IP
- Endereço MAC
- Primeira análise
- Última análise
- Vezes analisadas

Método de descoberta WAP

Você também pode configurar dispositivos gerenciados para escutar dispositivos de pontos de acesso wireless (WAP) na rede e adicionar dispositivos WAP descobertos ao grupo Wireless Access Points na ferramenta de Descoberta de dispositivos não gerenciados.

Para dispositivos WAP descobertos, XDD reporta a seguinte informação nas colunas de visualização de listagem:

- Nome do dispositivo
- Endereço MAC
- Primeira análise
- Última análise
- Vezes analisadas
- Status de WAP (Permitido, Enganoso, exceção Ativa)
- Fortaleza do sinal (use para determinar o local aproximado do dispositivo WAP)
- Nível de criptografia (o esquema de criptografia usado pelo dispositivo WAP)
- Fabricante

NOTA: Exibindo o endereço MAC
o XDD usa o API de detecção de rede sem fio dos dispositivos com Windows Vista e Windows 7 para obter o endereço MAC do dispositivo e exibi-lo no modo de exibição de listas. Porém, este recurso não é

compatível com dispositivos com o Windows XP.

Configuração de dispositivos para usarem a descoberta estendida de dispositivos (ARP e WAP)

Você pode usar a ferramenta de configuração de agentes para configurar alguns de seus dispositivos gerenciados com o agente da descoberta de dispositivos estendida (XDD) para que possam agir como dispositivos de descoberta que escutam por sinais de ARP e WAP na rede.

Não é necessário distribuir a descoberta estendida de dispositivo para cada dispositivo gerenciado, embora isso possa ser feito. A distribuição deste agente XDD para vários dispositivos em cada sub-rede deve dar a cobertura suficiente.

Para distribuir o agente da descoberta de dispositivos estendida para descoberta ARP e/ou WAP

1. Clique em **Ferramentas > Configuração > Configuração de agentes**.
2. Clique no botão da barra de ferramentas **Nova**.
3. Digite um **Nome de configuração**.
4. Na página **Descoberta de dispositivos estendida** da caixa de diálogo **Configuração de agentes**, selecione um ou ambos dos métodos de descoberta que deseja distribuir.
5. Especifique uma definição para o método de descoberta selecionado. Você pode selecionar uma definição existente da lista, ou clique em Configurar para editar uma definição ou criar uma nova para esta configuração de agentes.
6. Acabe a especificação de opções na configuração de agentes. Clique em **Ajuda** para obter mais informações sobre uma página.
7. Clique em **Salvar**.
8. Distribua a configuração de agentes aos dispositivos alvo desejados em cada subrede.

Você pode configurar vários parâmetros de descoberta estendida de dispositivo para dispositivos com o agente da descoberta estendida de dispositivo. Esse agente sincroniza periodicamente suas configurações com o servidor núcleo.

Para distribuir as configurações do agente da descoberta de dispositivos estendida para descoberta ARP e/ou WAP

1. Clique em **Ferramentas > Configuração > Descoberta de dispositivo não gerenciado**.
2. Clique no botão **Configurar descoberta de dispositivos estendida** da barra de ferramentas, e selecione o tipo de configuração do método de descoberta que deseja configurar (ARP ou WAP).
3. Especifique as opções de análise do método de descoberta. Para obter mais informações, clique em **Ajuda**.
4. Clique em **OK** ao terminar. Na próxima vez que os agentes de descoberta de dispositvos estendida sincronizarem com o servidor núcleo, as mudanças serão aplicadas.

Uso de relatórios de descoberta estendida de dispositivos

Vários relatórios XDD podem ser vistos na janela **Relatórios** (**Ferramentas > Relatórios / Monitoração**, clique em **Relatórios > Management Suite > Dispositivos não gerenciados**).

Relatórios da descoberta de dispositivos estendida incluem:

- **Histórico de dispositivos descobertos por ARP:** Histórico de dispositivos não autorizados.
- **Dispositivos descobertos por ARP atuais sem agente:** Dispositivos atuais onde o agente LANDesk está desativado ou não está funcionando.
- **Histórico de dispositivos descobertos por ARP sem agente:** Histórico de dispositivos onde o agente LANDesk está desativado ou não está funcionando.
- **Dispositivos não gerenciados:** Dispositivos na rede não designados ao servidor núcleo.
- **Dispositivos sem fio:** Histórico de todos os dispositivos sem fio que foram descobertos.

O que acontece quando um dispositivo é descoberto

Quando a UDD ou XDD localiza um dispositivo não gerenciado pela primeira vez, tenta identificar o tipo de dispositivo, de modo que possa adicionar o dispositivo a um dos seguintes grupos:

- **Computadores:** Contém dispositivos descobertos pelo método de análise UDD (e o método de descoberta ARP do agente XDD)
- **Resultado da pesquisa:** Contém os resultados da pesquisa.
- **Infra-estrutura:** Contém roteadores e outros hardwares de rede.
- **Intel vPro:** Contém dispositivos com Intel vPro ativado.
- **IPMI:** Contém servidores que têm a Intelligent Platform Management Interface.
- **Outro:** Contém dispositivos não identificados.
- **Impressoras:** Contém impressoras.
- **Hosts virtuais:** Contém hosts virtuais.
- **Pontos de acesso wireless:** Exibe dispositivos WAP descobertos (encontrados pelo agente XDD).

Esses grupos ajudam a manter a lista da UDD organizada de forma que você possa localizar com mais facilidade os dispositivos nos quais tem interesse. É possível ordenar as listas de dispositivos por qualquer cabeçalho de coluna clicando em um dos cabeçalhos.

NOTA: Movendo dispositivos para grupos diferentes
A UDD pode não categorizar os dispositivos corretamente e colocá-los nos grupos de dispositivos apropriados cada vez. Se isto acontecer, os dispositivos identificados incorretamente podem ser arrastados com facilidade até o grupo correto.

A UDD tenta descobrir e relatar informação básica sobre cada dispositivo, incluindo os dados seguintes que aparecem na visualização de listagem do item no painel direito da janela ferramentas:

- **Nome do dispositivo:** nome do dispositivo descoberto, se disponível.
- **Endereço IP:** endereço IP descoberto. Isso é sempre mostrado pela UDD. XDD não.
- **Máscara de sub-rede:** a máscara de sub-rede descoberta. Isso é sempre mostrado pela UDD.
- **Descrição de SO:** descrição do SO descoberto, se disponível.
- **Endereço MAC:** O endereço MAC descoberto, normalmente retornado se o dispositivo tiver o agente LANDesk padrão, NetBIOS ou se o dispositivo estiver na mesma sub-rede que o servidor núcleo ou o console que está fazendo a descoberta.
- **Grupo:** O grupo da UDD ao qual o dispositivo pertence.
- **Agente LANDesk padrão:** Mostra se o dispositivo está com o CBA carregado. Você pode distribuir outros agentes LANDesk diretamente para dispositivos gerenciados com o CBA carregado.

- **Todos os usuários:** Usuários conectados ao dispositivo que está sendo analisado, se estiver disponível.
- **Grupo/Domínio:** O grupo/domínio do qual o dispositivo é um membro, se estiver disponível.
- **Primeira varredura:** A data em que a UDD fez a primeira varredura deste dispositivo.
- **Última varredura:** A data em que a UDD fez a última varredura deste dispositivo. Essa coluna ajuda a localizar dispositivos não gerenciados que podem não estar mais na rede ou que foram localizados recentemente.
- **Número de varreduras:** O número de vezes que a UDD analisou este dispositivo.
- **Descobertos por ARP:** Se oi dispositivo foi descoberto através de ARP.
- **Exceção XDD:** Se o dispositivo é uma exceção XDD.
- **GUID IPMI:** O GUID IPMI do dispositivo, se disponível.

Dependendo do dispositivo, a UDD pode não ter informações em todas as colunas. Quando a UDD localiza um dispositivo pela primeira vez, ele verifica no banco de dados núcleo se o endereço IP e o nome do dispositivo já estão no banco de dados. Caso haja uma correspondência, a UDD ignorará o dispositivo. Caso não haja uma correspondência, a UDD adicionará o dispositivo à tabela de dispositivos não gerenciados. Os dispositivos na tabela não gerenciados não usam uma licença LANDesk. Um dispositivo é considerado gerenciado quando envia uma análise de inventário ao banco de dados núcleo. Não é possível arrastar dispositivos da UDD para a tela de rede do console principal. Quando os dispositivos não gerenciados submetem uma varredura de inventário eles serão removidos da UDD e adicionados à tela de rede automaticamente.

É possível criar grupos personalizados para classificar ainda mais os dispositivos não gerenciados. Se você mover um dispositivo para outro grupo, a UDD deixará esse dispositivo nesse grupo se a UDD detectar o dispositivo novamente mais tarde. Mantendo o grupo principal **Computadores** organizado e movendo os dispositivos que você sabe que não serão gerenciados pelo LANDesk em subgrupos ou em outras categorias, é possível ver facilmente novos dispositivos no grupo **Computadores**. Se você excluir um grupo que possui dispositivos, a UDD transferirá os dispositivos para o grupo **Outro**.

Se você quiser excluir todos os dispositivos de grupos múltiplos grupos de uma só vez, clique no botão da barra de ferramentas **Excluir itens em grupos** e selecione os grupos dos quais você quer excluir todos os dispositivos.

É possível localizar com rapidez dispositivos que atendam aos critérios da pesquisa que você especifica usando o campo da barra de ferramentas **Localizar**. Você pode pesquisar informações em uma determinada coluna ou em todas as colunas. Os resultados da pesquisa são exibidos na categoria **Resultados da pesquisa**. Por exemplo, use Localizar para agrupar computadores não gerenciados que tenham CBA, pesquisando por "S" no campo do agente LANDesk padrão.

Você pode também criar um alerta quando a UDD localizar dispositivos não gerenciados. Em Alertas (**Ferramentas > Configuração > Alertas**, clique em **Conjunto de alertas de núcleo**) o nome do alerta a configurar é **Descoberta de dispositivo não gerenciado - dispositivo não gerenciado encontrado**.

Trabalhar com dispositivos encontrados com XDD

Dispositivos não gerenciados encontrados através do método de descoberta ARP da descoberta de dispositivos estendida aparecem na lista **Computadores** da janela **Descoberta de dispositivos não gerenciados**. Dispositivos WAP encontrados através do método de descoberta WAP da descoberta de dispositivos estendida aparecem na lista **Pontos de acesso wireless** da janela **Descoberta de dispositivos não gerenciados**.

Destas listas você pode executar as opções normais de UDD como, por exemplo, transferi-los para outros grupos. Clique com o botão direito em um dispositivo para acessar o menu de atalho e usar as opções disponíveis.

Você pode também importar e exportar exceções de descoberta estendida de dispositivo. Uma exceção é um dispositivo na rede o qual não é gerenciado ou que é conhecido pelo administrador, mas que ele não quer que seja reportado pela descoberta estendida de dispositivo.

Essas exceções estão em formato de arquivo de texto CSV que consistem em endereços IP e MAC separados por vírgula nessa ordem, um par por linha. As exportações de exceções incluem todas as exceções armazenadas no banco de dados. As importações de exceções substituem todas as exceções armazenadas no banco de dados com as exceções contidas no arquivo importado.

Exportar e importar exceções de descobertas

Para exportar todas as exceções de descoberta estendida de dispositivo

1. Clique em **Ferramentas > Configuração > Descoberta de dispositivo não gerenciado**.
2. Clique no botão da barra de ferramentas **Exportar exceções de descoberta estendida de dispositivo para arquivo CSV**.
3. Escolha uma pasta e dê um nome ao arquivo.
4. Clique em **Salvar**.

Para importar todas as exceções de descoberta estendida de dispositivo

1. Crie ou atualize um arquivo CSV separado por vírgula que contém as exceções que deseja.
2. Clique em **Ferramentas > Configuração > Descoberta de dispositivo não gerenciado**.
3. Clique no botão da barra de ferramentas **Importar exceções de descoberta estendida de dispositivo do arquivo CSV**.
4. Selecione o arquivo CSV e clique em **Abrir**.

Resolução de problemas de resultados imprecisos de versão de SO

Em alguns ambientes, um mapeamento de nmap em um endereço IP que não está em uso retorna uma resposta sobre portas específicas, confundindo o nmap. As portas que respondem ou não respondem variam em diferentes ambientes. Se o nmap não retornar resultados de versão de SO precisos ou como melhor prática, o nmap deve ser ajustado para o ambiente do cliente.

Para ajustar o nmap

1. Determine vários endereços IP que não estão em uso no ambiente.
2. No prompt de comando no servidor núcleo, use a linha de comando a seguir para analisar manualmente os endereços IP:

   nmap -O -sSU -F -T4 -d -v <targets> -oX test.xml > test.txt

3. Revise os resultados e veja se há alguma porta respondendo consistentemente nos endereços IP que não estão em uso.

4. Abra o documento de serviços nmap do Management Suite (C:\Arquivos de programas\LANDesk\Management Suite\nmap\nmap-services) e coloque as portas que estão respondendo Consistentemente, dentro de comentários com caracteres hash #.

Ajuda da descoberta de dispositivos não gerenciados

A ferramenta Descoberta de dispositivos não gerenciados (UDD) da LANDesk é acessível do console principal do LANDesk (**Ferramentas > Configuração > Descoberta de dispositivos não gerenciados**). Use esta ferramenta para localizar dispositivos na sua rede, os quais não enviaram uma varredura de inventário ao banco de dados núcleo LANDesk. A UDD tem várias formas de localizar dispositivos não gerenciados. Esta ferramenta também suporta descoberta de dispositivos estendida (XDD), que depende de um agente de dispositivo que está alerta para difusões de redes WAP e ARP. O agente de descoberta de dispositivos estendida checa os dispositvos descobertos para ver se têm o agente LANDesk. Se o agente LANDesk não responder, a descoberta de dispositivo estendido mostra o dispositivo na lista **Computadores**. A descoberta estendida de dispositivo é ideal nas situações que envolvem firewalls as quais impedem os dispositivos de responderem aos métodos de descoberta UDD baseada em ping.

Esse capítulo contém as seções de ajuda online a seguir que descrevem as caixas de diálogo da ferramenta Descoberta de dispositivos não gerenciados. Na interface do console, esses tópicos de ajuda são acessados clicando no botão **Ajuda** em suas respectivas caixas de diálogo.

Sobre a caixa de diálogo Configuração da análise

Use esta caixa de diálogo para personalizar e iniciar análises de dispositivos não gerenciados. Para acessar esta caixa de diálogo, na janela da ferramenta **Descoberta de dispositivos não gerenciados**, clique no botão da ferramenta **Analisar rede**.

- **Configurações salvas:** Mostra as configurações do analisador salvas. Salve uma configuração alterando as definições desejadas, em seguida clique em **Novo**, nomeie a configuração e, com a nova configuração selecionada, clique em **Salvar**.
- **Mais >>:** Expande a caixa de diálogo para mostrar opções de descoberta.
- **Análise de rede:** Descobre dispositivos usando uma análise de ping ICMP. Esse é o método de descoberta mais completo e recomendado.
    - **Impressão digital de SO de IP:** Um nível adicional de descoberta que usa respostas de pacote para tentar determinar o SO instalado no dispositivo descoberto.
    - **Usar SNMP:** Um nível adiciona de descoberta que usar SNMP para deteção de dispositivo.
- **Discobre dispositivos com LANDesk CBA instalado:** Descobre dispositivos com o agente CBA em execução. Caso seus dispositivos tenham o CBA, esse será o método de descoberta mais rápido.
    - **Descobre dispositivos com LANDesk PDS2 instalado:** Descobre dispositivos usando o agente do PDS2 LANDesk mais antigo. Essa opção só poderá ser selecionada se **Descobrimento do CBA** já estiver selecionado.
- **Descobre dispositivos usando domínio NT:** Descobre dispositivos em um domínio do Windows NT. Essa opção usa informações da conta do domínio de NT e não exige um intervalo de endereço IP, embora você possa especificar um. Selecione esta opção e clique em **Configurar** para exibir a caixa de diálogo **Configuração do domínio do NT**. Nesta caixa de diálogo você pode personalizar as configurações da descoberta no domínio do NT.
- **Filtro por intervalo de IP** (para o domínio de NT e LDAP): Filtra o descoberta do domínio de NT e de LDAP nos intervalos de IP especificados em **IP inicial** e **IP final**.

- **Descobre dispositivos usando LDAP:** Descobre dispositivos em um diretório LDAP. Selecione esta opção e clique em **Configurar** para exibir a caixa de diálogo **Configuração do LDAP**. Nesta caixa de diálogo você pode personalizar as configurações da descoberta LDAP.
- **Descobre dispositivos com o IPMI ativado:** Procura os servidores habilitados com o IPMI - Intelligent Platform Management Interface, o que permite que você acesse muitos dos recursos do servidor, independentemente de o servidor estar ligado ou desligado ou do estado no qual o SO se encontra.
- **Descobrir hosts virtuais:** procura servidores executando VMware ESX Server.
- **IP inicial:** digite o endereço IP inicial do intervalo de endereços a ser analisado.
- **IP final:** digite o endereço IP final do intervalo de endereços a ser analisado. A UDD atualiza esse campo automaticamente, à medida que você digita o **IP inicial**, mas é possível mudar o endereço IP final manualmente. O **IP final** é calculado usando-se o valor da **Máscara da sub-rede** + o que for digitado em **IP inicial**.
- **Máscara de sub-rede:** Digite a máscara da sub-rede do intervalo do endereços IP que está sendo analisado.
- **Adicionar** e **Remover:** Adiciona ou remove os intervalos de endereços IP da fila de trabalho, na parte inferior da caixa de diálogo.
- **Agendar tarefa:** Agenda a varredura com base em suas configurações. Você pode personalizar a hora inicial na janela **Tarefas agendadas**. As varreduras agendadas originam-se do servidor núcleo.
- **Executar análise agora:** Inicia a análise imediatamente com base em suas configurações. As análises iniciadas aqui originam-se do console em que você está. Depois de iniciar a análise, uma caixa de diálogo **Status da análise** é exibida mostrando o número total de dispositivos localizados, quantos dispositivos existentes foram atualizados e quantos dispositivos não gerenciados novos foram adicionados.

Sobre a caixa de diálogo Configuração do domínio do NT

Use essa caixa de diálogo para configurar como se conectar ao domínio a ser analisado.

- **Domínio:** Digite o domínio a ser analisado.
- **Login como usuário atual:** Selecione essa opção se estiver conectado como um usuário com acesso ao domínio que está analisando.
- **Fazer login como.** Selecione essa opção se não estiver conectado como um usuário com acesso ao domínio que está analisando. Além disso, digite um **Nome de usuário** e uma **Senha**.
- **Usar info do domínio:** Usa informações do domínio sobre o SO detectado do dispositivo.
- **Adicionar** e **Remover:** Adicione cada domínio que foi configurado e que deseja analisar à fila de trabalho clicando em **Adicionar**. Clique em **Remover** para excluir o domínio selecionado da fila de trabalho.

Sobre a caixa de diálogo Configuração do LDAP

Use essa caixa de diálogo para configurar como se conectar ao diretório LDAP a ser analisado.

- **LDAP://:** Informe o diretório LDAP a ser analisado.
- **Login como usuário atual:** Selecione essa opção se estiver conectado como um usuário com acesso ao diretório que está analisando.
- **Fazer login como.** Selecione essa opção se não estiver conectado como um usuário com acesso ao diretório que está analisando. Além disso, digite um **Nome de usuário** e uma **Senha**.

- **Selecionar OUs individuais:** Selecione as OUs a serem analisadas. Clique em **Adicionar** para adicioná-las à fila de trabalho. Clique em **Remover** para excluir a OU selecionada da fila.
- **Caminho do Active directory:** Mostra o caminho do Active directory, se aplicável.

Configuração de análises SNMP

As descobertas de análise de rede podem usar SNMP. Dependendo da sua configuração SNMP da rede, pode ser necessário digitar informações opcionais de SNMP em UDD. Se a opção **Configurar** próxima à opção **SNMP** for selecionada, a caixa de diálogo **Configuração SNMP** será mostrada com as seguintes opções:

- **Novas tentativas:** número de vezes de tentativas de UDD para a conexão SNMP.
- **Aguardar pela resposta em segundos:** Tempo que a UDD de aguardar para um resposta SNMP.
- **Porta:** A porta onde a UDD deve enviar as consultas SNMP.
- **Nome de comunidade:** Nome da comunidade SNMP que a UDD de usar.
- **Configurar SNMP V3:** a UDD também suporta SNMP V3. Clique neste botão para configurar as opções SNMP V3 na caixa de diálogo **Configuração de SNMP V3**

A caixa de diálogo **Configuração SNMP V3** possui as seguintes opções:

- **Nome de usuário:** O nome de usuário que a UDD deve usar para autenticar-se com o serviço SNMP remoto.
- **Senha:** A senha para o serviço SNMP remoto.
- **Tipo de autenticação:** O tipo de autenticação usado pelo SNMP. Pode ser **MD5**, **SHA** ou **Nenhum**.
- **Tipo** de privacidade: método de criptografia usado pelo serviço SNMP. Pode ser **DES**, **AES128** ou **Nenhum**.
- **Senha** de privacidade: senha a ser usada com o tipo especificado de privacidade. Não estará disponível se você selecionar o tipo de privacidade **Nenhum**.

Sobre o diálogo Lista das configurações da descoberta ARP (ou WAP)

Use esta caixa de diálogo para gerenciar as configurações ARP e WAP usadas para a descoberta de dispositivos estendida. Quando configuradas, você poderá aplicar as definições de XDD às tarefas de análise.

Esta caixa de diálogo contém as seguintes opções:

- **Novo:** Abre a caixa de diálogo configurações onde poderá definir as opções do método de descoberta.
- **Editar:** Abre a caixa de diálogo de definições onde você pode modificar a configuração selecionada.
- **Copiar:** Abre uma cópia da configuração selecionada como um modelo que pode ser modificado e renomeado. Isso é útil quando você deseja fazer pequenos ajustes nas configurações e salvá-los para um fim específico.
- **Excluir:** remove a configuração selecionada do banco de dados.
  Observe que a configuração selecionada pode estar associada no momento com uma ou mais tarefas ou dispositivos gerenciados. Se você decidir excluir as configurações, os dispositivos com aquelas definições ainda a reterão e continuarão a usá-las até que uma tarefa de configuração de novo agente seja distribuída; as tarefas agendadas com aquelas configurações ainda serão executadas nos dispositivos alvo, assim como as tarefas do agendador local com aquelas configurações até que uma nova configuração seja distribuída.
- **Fechar:** fecha a caixa de diálogo sem aplicar uma configuração à tarefa.

Sobre a caixa de diálogo Configurar as definições da descoberta ARP

Use este diálogo (botão **Configurar descoberta estendida de dispositivo** da barra de ferramentas> **Configurar definições de descoberta ARP**) para personalizar definições de análise de descoberta estendida baseada.

- **Nome de configuração:** Identifica a definição com um nome exclusivo. Esse nome é exibido na lista suspensa de configurações na caixa de diálogo lista de configurações.
- **Estatísticas de entrada de ARP de duração em cache (em segundos):** Por quanto tempo os dispositivos com agente de descoberta estendida de dispositivo mantêm um endereço na tabela de ARP. Não será mais feito ping aos dispositivos no cache da ARP após o ping de descoberta inicial. O valor padrão é 24 horas (86.400 segundos). O valor mínimo é 900 segundos.
- **Demora máxima antes de ser feito o ping de um dispositivo desconhecido para o agente LANDesk (em segundos):** Quando um novo ARP é reconhecido por um dispositivo com o agente de descoberta de dispositivos estendida, o dispositivo aguarda dois minutos para o dispositivo detectado inicializar e, a seguir, aguarda um tempo aleatório dentro do valor que você especificar. O agente com a espera aleatória mais curta faz o ping primeiro e, a seguir, a difusão de UDP para a sub-rede que cuidou do ping para aquele dispositivo. Se você tiver vários agentes de descoberta estendida de dispositivo instalados, isso impede os dispositivos de gerarem tráfego em excesso se todos fizerem ping ao mesmo tempo. Se você definir esse valor muito alto, os dispositivos não gerenciados podem sair da rede antes que seja feito ping a eles. Se você definir esse valor muito baixo, os agentes variados podem fazer ping e reportar o mesmo dispositivo. O valor padrão é uma hora (3.600 segundos).
- **A freqüência de tabela de ARP em cache é atualizada (em segundos):** Qual é a freqüência com que o dispositivo grava o cache de ARP no disco para os dados não serem perdidos em caso de o dispositivo ser desligado, cair ou reinicializar. O valor padrão é de cinco minutos (300 segundos).
- **Nível de login:** O nível de login local de descoberta de dispositivos estendidos para erros (1), aviso (2), tudo (3). O nível padrão é 1- somente erros. Os logs são armazenados localmente no arquivo C:\Arquivos do programa\LANDesk\LDClient\xddclient.log.
- **Forçar nível de login:** Sobrepassa a configuração de nível de log do servidor núcleo. Se desmarcar esta opção, você pode definir o nível de log manualmente em um dispositivo em particular. Isso pode ser útil para a solução de problemas em um dispositivo específico sem precisar mudar o nível de log em todos os dispositivos. Isso é habilitado como padrão.

Sobre a caixa de diálogo Configurar as definições da descoberta WAP

Use esta caixa de diálogo (botão **Configurar descoberta estendida de dispositivo** da barra de ferramentas> **Configurar definições de descoberta WAP**) para personalizar definições de análise de descoberta estendida baseada em WAP.

Esta caixa de diálogo contém as seguintes opções:

- **Nome de configuração:** Identifica a definição com um nome exclusivo. Esse nome é exibido na lista suspensa de configurações na caixa de diálogo lista de configurações.
- **Freqüência da análise WAP (em segundos):** Especifica a freqüência com que o agente da descoberta de dispositivos estendida analisa por pontos WAP.
- **Nível de login:** O nível de login local de descoberta de dispositivos estendidos para erros (1), aviso (2), tudo (3). O nível padrão é 1- somente erros. Os logs são armazenados localmente no arquivo C:\Arquivos do programa\LANDesk\LDClient\xddclient.log.

- **Forçar nível de login:** Sobrepassa a configuração de nível de log do servidor núcleo. Se desmarcar esta opção, você pode definir o nível de log manualmente em um dispositivo em particular. Isso pode ser útil para a solução de problemas em um dispositivo específico sem precisar mudar o nível de log em todos os dispositivos. Isso é habilitado como padrão.

Sobre a caixa de diálogo de histórico de descoberta ARP

Use esta caixa de diálogo (botão **Configurar histórico de descoberta ARP** da barra de ferramentas) para configurar a maneira como o servidor mantém o histórico de descoberta ARP. Estes dados históricos são usados para a geração de relatórios de descoberta estendida de dispositivo. As opções neste diálogo não afetam os dispositivos descobertos que aparecem na janela principal de descoberta de dispositivos não gerenciados. Este histórico só se aplica a dispositivos que foram descobertos através da descoberta ARP e que não têm agentes LANDesk.

- **Manter o histórico por este período, em dias:** Esta opção permite especificar o número de dias de dados do histórico da descoberta ARP que você quer salvar no banco de dados. Os dados de histórico de descoberta ARP mais antigos que o número de dias que você especificar serão apagados do banco de dados durante a manutenção.
- **Limpar entradas manualmente:** Este é o padrão. O histórico de descoberta ARP não será excluído durante a manutenção.
- **Limpar todas as entradas agora:** Clique neste botão para apagar imediatamente o histórico de descoberta ARP do banco de dados.

Distribuição do SO

Visão geral da distribuição do SO

A ferramenta de distribuição de SO LANDesk agrupa vários recursos que lhe permite distribuir imagens para dispositivos novos e existentes. Estas características dinamizam o provisionamento do novo dispositivo e a redistribuição de dispositivos existentes. Você também pode migrar perfis de usuário e distribuir imagens com modelos independentes de hardware que podem ser aplicados à modelos de dispositivos diferentes.

Com esses recursos automatizados que você pode distribuir e recriar as imagens nos dispositivos sem a interação do usuário ou a necessidade de um técnico ter que trabalhar em cada dispositivo. Você pode agendar distribuições e migrações para depois do expediente. Ao usar a tecnologia LANDesk® Targeted Multicast™ para distribuir imagens, você não saturará a largura de banda da rede ao distribuir a mesma imagem para vários dispositivos.

Os seguintes recursos são parte da ferramenta de distribuição de SO:

- **Distribuição do SO:** Cria imagens e scripts para distribuir imagens em ambientes de pré-inicialização do DOS e Windows. Use a distribuição baseada em agente ou em PXE para distribuir imagens.
- **Geração de imagem independente de hardware:** Cria um modelo de geração de imagem que é independente de hardware para que você possa aplicar uma modelo a dispositivos de múltiplos fabricantes. Crie um repositório de drivers; os drivers que se aplicam a cada dispositivo são injetados durante os processos de criação de geração de imagem.
- **Provisionamento:** Cria modelos que aplicam uma faixa completa de atributos e recursos de dispositivo ao processo de criação de geração de imagem. Além de distribuir imagens de SO, você pode definir ações que ocorrem antes e depois do SO ser instalado, como instalação de software, patch de sistema e configuração de unidade e de parâmetros de rede. Você pode provisionar novos dispositivos e prepará-los para uso no seu ambiente sem tempo ocioso.
- **Migração de perfil:** Captura e restaura os dados de perfil do usuário quando você atualiza um computador de usuário ou os atribui a um novo núcleo. Você pode preservar a área de trabalho do usuário, as configurações de aplicativo, configurações de impressora e rede e a estrutura de arquivos e pastas no novo dispositivo.

Tópicos relacionados

"Distribuição baseada no agente" na página 376

"Visão geral do Distribuição baseada no PXE" na página 368

"Visão geral da imagem independente de hardware" na página 381

"Provisionamento" na página 423

"Visão geral da migração de perfil" na página 385

Usar a distribuição do SO para distribuir imagens

O recurso de distribuição de SO (OSD) oferece dois métodos de distribuição de imagens do SO para dispositivos na rede:

- **Distribuição baseada no agente:** Usa o SO existente do Windows do dispositivo e agentes LANDesk instalados para distribuir imagens.

- **Distribuição baseada no PXE:** permite criar a imagem para dispositivos com discos rígidos vazios ou SOs que não foram usados. Os representantes PXE leves eliminam a necessidade de um servidor PXE dedicado em cada sub-rede.

Se o utilitário Sysprep da Microsoft for usado para criar imagens, a distribuição do SO criará arquivos sysprep.inf personalizados e os inserirá em cada imagem do dispositivo por cliente, personalizando os nomes dos computadores no Windows, informações de domínio etc, no banco de dados núcleo.

A distribuição do SO inclui uma ferramenta de criação de geração de imagem incorporada que pode ser usada para criar imagens. A distribuição do SO também oferece suporte a ferramentas de criação de geração de imagem de outros fabricantes que já podem estar em uso como, Symantec Ghost, PowerQuest DeployCenter e Microsoft XImage.

A distribuição de SO pode criar imagem, distribuir e migrar usando os seguintes ambientes de inicialização:

- DOS
- Windows PE*

* O Kit de ferramentas LANDesk PE usa o software Microsoft Windows Pre-installation Environment (“WinPE”), um produto de terceiros. Para usar o Kit de ferramentas LANDesk® PE, você deve ter aceito o contrato de licença da Microsoft para o WinPE.

O uso do ambiente DOS PE exigem software licenciado, portanto será necessário fornecer cópias do software licenciado para serem validadas pela distribuição de SO antes de poder usar o ambiente específico.

AVISO: A distribuição do SO (geração de imagem) deve ser usada com cautela. A distribuição do sistema operacional inclui a limpeza de todos os dados existentes no disco rígido do dispositivo e a instalação de um novo sistema operacional. Haverá um grande risco de perda de dados críticos se a distribuição do SO não for executada exatamente segundo descrito neste documento ou se imagens pouco implementadas forem usadas. Antes de executar qualquer distribuição do SO, recomendamos fazer backup de todos os dados para que, se houver alguma perda de dados, ela possa ser recuperada.

Etapas de distribuição de SO para dispositivos Windows

Ao planejar e implementar uma operação de distribuição do SO Windows, siga esta seqüência de etapas:

1. Se planejar usar um ambiente de geração de imagem DOS ou Windows PE e não tiver validado suas licenças ainda, clique no botão da barra de ferramentas **Validar licenças** na janela **Distribuição de sistema operacional**. O Windows PE está instalado para você como parte da instalação do Management Suite. Antes de usar o Ambiente do Windows PE, você deve aceitar os termos da licença (clique no botão **Licença** primeiro e leia a nota importante abaixo antes de começar). Para DOS PE, clique em **Validar agora** e insira os CDs do sistema operacional conforme solicitado. Só é necessário fazer isso uma vez.
2. (Opcional) Execute os utilitários Gerenciador de instalação e Sysprep da Microsoft no dispositivo cuja imagem será capturada.
3. Crie ou reutilize um script de captura de imagem na janela **Distribuição de sistema operacional**.
4. Agende uma tarefa por meio da ferramenta **Tarefas agendadas** que executa o script de imagem de captura no dispositivo cuja imagem será capturada. (Observe as atualizações da janela **Status da tarefa personalizada** para ver se houve êxito ou falha.)
5. Crie ou reutilize um script existente de distribuição de captura de imagem na janela **Distribuição de sistema operacional**.

6. Agende uma tarefa por meio da ferramenta **Tarefas agendadas** que executará o script de imagem de distribuição nos dispositivos alvo cuja imagem será distribuída.
7. Os dispositivos alvo que executam SOs Windows e agentes do LANDesk iniciarão a tarefa de distribuição de imagem conforme agendado (distribuição baseada no agente).
8. Os dispositivos alvo habilitados para PXE iniciarão a tarefa de distribuição de imagem na próxima inicialização (distribuição baseada no PXE).

IMPORTANTE: Este produto instala componentes do Windows Automated Installation Kit (WAIK) para Windows 7 como parte da instalação do produto, que inclui um Ambiente do Windows PE. Não instale qualquer outra versão do WAIK no servidor núcleo ou haverá conflitos entre as duas versões do WAIK. Se você quiser usar qualquer outra versão do WAIK, instale-o em outro dispositivo, diferente do servidor núcleo.

Etapas de distribuição de SO para dispositivos Linux

A seguir, está uma lista das restrições impostas nas instalações Linux.

1. A partição ('/') da raiz deve ser do tipo de sistema de arquivos ext2, ext3, ou xfs.
2. A partição raiz *não pode* estar contida em um LVM PV (Logical Volume Manager - Physical Volume), mas *precisa* ser uma partição (física ou extendida) no MBR (Master Boot Record) da unidade.
3. A última partição é a única que pode ser expandida; assim sendo, deve também ser do tipo de sistema de arquivo ext2, ext3, ou xfs.
4. Você deve especificar a localização da partição da raiz (isto é, hda3 ou sda2)

Ao planejar e implementar uma operação de distribuição do SO Linux, siga esta seqüência de etapas:

1. Crie ou reutilize um script de captura de imagem na janela **Distribuição de sistema operacional**.
2. Agende uma tarefa por meio da ferramenta **Tarefas agendadas** que executa o script de imagem de captura no dispositivo cuja imagem será capturada. (Observe as atualizações da janela **Status da tarefa personalizada** para ver se houve êxito ou falha.)
3. Crie ou reutilize um script de distribuição de imagem de configuração Linux com o assistente **Distribuição do SO/Tarefas de migração**.
4. Agende uma tarefa por meio da ferramenta **Tarefas agendadas** que executará o script de imagem de distribuição nos dispositivos alvo cuja imagem será distribuída.
5. Os dispositivos alvo que executam SOs Windows e agentes do LANDesk iniciarão a tarefa de distribuição de imagem conforme agendado (distribuição baseada no agente).
6. Os dispositivos alvo habilitados para PXE iniciarão a tarefa de distribuição de imagem na próxima inicialização (distribuição baseada no PXE).

Diretrizes da imagem do SO

É possível criar imagens do SO por meio da ferramenta de criação de geração de imagem do ou outras ferramentas de criação. Quando o assistente de Distribuição do SO/Tarefas de migração é executado para criar um script de criação de geração de imagem, será necessário especificar o tipo de geração de imagem e a ferramenta de criação de geração de imagem. O assistente gera automaticamente linhas de comando para a ferramenta de geração de imagem do LANDesk (ImageW) e para o Microsoft ImageX, mas não para o Symantec Ghost ou outras ferramentas de imagem.

NOTA: Ao instalar o componente da distribuição do SO e da migração de perfil, os arquivos para a ferramenta de geração de imagem do LANDesk são automaticamente instaladas no servidor núcleo. Se desejar executar a ferramenta de geração de imagem do LANDesk a partir de um local diferente, será necessário copiar esses quatro arquivos: imageall.exe, image.exe, restall.bat, and backall.bat. Se quiser usar o Microsoft ImageX, você deve copiar os arquivos ximage.exe and xmlrw.dll na pasta \\<core>\ManagementSuite\OSD\imaging.

Se você tiver uma ferramenta de criação de geração de imagem diferente, poderá fornecer a linha de comando para ela no final do assistente. Se você especificar uma linha de comando personalizada, o assistente colocará a linha personalizada no local correto no script, portanto não será necessário editar o script manualmente.

Ambientes de criação de geração de imagem de distribuição de SO

Ao capturar ou restaurar uma imagem, a distribuição de SO inicializa o dispositivo alvo em um ambiente de criação de imagens. A distribuição de SO suporta os seguintes ambientes de criação de imagens:

- **DOS**: A verificação da licença exige o CD de servidor Windows NT 4 e o CD Windows 98. Esta imagem é a menor, o que reduz a largura de banda de rede usada. É potencialmente mais lenta na criação e restauração de imagens e apresenta menor compatibilidade de hardware que o Windows PE.
- **Windows PE**: A licença é incluída neste produto. Esta imagem é a maior. Ela apresenta a melhor compatibilidade de hardware e é, potencialmente, a criação e restauração mais rápida de imagens. A velocidade da geração de imagem beneficia-se dos drivers e aplicativos de 32 bits. Este ambiente de criação de geração de imagem também suporta as ferramentas de geração de imagem da Microsoft.

Observe que o ambiente de criação de imagens que você escolher é independente do SO cuja imagem está sendo criada. Por exemplo, você pode usar o ambiente de geração de imagem Windows para criar imagens de sistemas operacionais Linux.

Nomes de arquivos de imagem

Você deve dar às imagens nomes de arquivos exclusivos. Poderão ocorrer problemas se imagens diferentes com o mesmo nome de arquivo forem distribuídas simultaneamente na mesma sub-rede. Dependendo de como um utilitário de criação de geração de imagem nomear arquivos de geração de imagem e do ambiente de criação de geração de imagem utilizado (por exemplo, DOS com imagens Ghost com vários arquivos), o arquivo poderá ter somente cinco caracteres únicos depois da conversão para um formato de nome do DOS 8.3.

Ao capturar imagens, a ferramenta de imagens LANDesk para DOS, Windows e Linux utiliza os últimos seis caracteres do nome do computador, seguido pelo número de dois dígitos da imagem para cada arquivo na imagem. Se estiver capturando imagens de vários dispositivos ao mesmo tempo e os últimos seis caracteres do nome do computador não forem exclusivos, ocorrerá erros durante o processo de captura.

O Symantec Ghost usa, em geral, os primeiros oito caracteres do nome do computador para criar o nome de arquivo da imagem, o que deve também ser exclusivo para as capturas de imagens simultâneas funcionarem.

Ao capturar imagens de vários dispositivos, há dois meios para garantir que elas tenham nomes exclusivos:

- criar a imagem de um dispositivo por vez, renomeando cada uma conforme é criada;
- Antes de executar uma tarefa, verifique se os últimos seis caracteres (ferramenta de imagens LANDesk) ou os primeiros oito caracteres (Symantec Ghost) do nome do computador Windows são exclusivos.

LANDesk agentes e imagens

Não inclua os agentes LANDesk em imagens. Se você usar uma imagem Sysprep, a distribuição do SO instalará os agentes LANDesk no SO Windows após a imagem ser restaurada.

Se suas imagens não-Sysprep baseadas no Windows incluírem agentes LANDesk, será necessário excluir o arquivo ldiscan.cfg da raiz do disco rígido antes de criar a imagem. Será necessário também excluir as seguintes chaves:

- HKLM\Software\Intel\LANDesk\Common API\Unique ID
- HKLM\Software\LANDesk\Common API\Unique ID

Se você deixá-los na imagem, todos os dispositivos que usarem a imagem terão a mesma entrada no banco de dados núcleo. Como alternativa, se houver imagens não-Sysprep com agentes LANDesk, será possível habilitar a opção **Rejeitar identidades duplicadas** na caixa de diálogo **ID de dispositivo duplicado** (**Configurar > Serviços > Inventário > IDs do dispositivo)**.

Partições e imagens

Por padrão, quando a distribuição do SO restaura uma imagem em um dispositivo alvo, ela exclui quaisquer partições existentes naquele cliente.

A ferramenta de criação de geração de imagem LANDesk suporta imagens de partição única e também de várias partições (até quatro partições).

Imagens não-Windows

É possível usar a distribuição do SO para distribuir quase qualquer imagem com suporte da ferramenta de criação de geração de imagem, não apenas imagens baseadas no Windows. Ao distribuir imagens não-Windows ou não-Sysprep, não selecione a opção **A imagem é Sysprepped** nas caixas de diálogo da nova configuração.

Validação de licenças para ambientes de imagem

Ao capturar ou restaurar uma imagem, a distribuição de SO inicializa o dispositivo alvo em um ambiente de criação de imagens. A distribuição de SO é compatível com dois ambientes de imagens (DOS, Windows). Você precisa validar sua licença para usar o ambiente DOS PE e você precisa aceitar a licença para o ambiente Windows PE que é instalada com este produto.

Para validar um ambiente DOS PE

1. Clique no botão **Validar licenças** na barra de ferramentas.
2. Na seção **Ambiente de imagem DOS** clique em **Validar agora**.
3. Insira um CD de instalação de servidor Windows NT4 em uma unidade. Clique em **Procurar** e selecione a pasta \CLIENTS\MSCLIENT\DISKS no CD.
4. Clique em **OK**. O processo de validação acessa arquivos nesse CD. Quando terminar, ele avisa para colocar o próximo CD.
5. As ser solicitado, insira um CD de instalação do Windows 98 em uma unidade. Clique em **Procurar** e selecione a pasta \WIN98 no CD.
6. Clique em **OK**. O processo de validação continuará e quando terminar, clique em **OK**.

Para aceitar a licença para o Ambiente do Windows PE

1. Clique no botão **Validar licenças** na barra de ferramentas.
2. Na seção **Contrato de licença do Windows PE**, clique em **Licença**.
3. Clique no link para aceitar os termos da licença WAIK. A mensagem "Aceito" é exibida na caixa de diálogo Ambiente de imagem OSD.

IMPORTANTE: Este produto instala componentes do Windows Automated Installation Kit (WAIK) para Windows 7 como parte da instalação do produto, que inclui um Ambiente do Windows PE. Não instale qualquer outra versão do WAIK no servidor núcleo ou haverá conflitos entre as duas versões do WAIK. Se você quiser usar qualquer outra versão do WAIK, instale-o em outro dispositivo, diferente do servidor núcleo.

Selecionar um ambiente de pré-inicialização padrão

A caixa de diálogo de validação permite que você modifique o Ambiente de pré-inicialização padrão para dispositivos na fila de espera PXE. Os dispositivos na fila de espera serão inicializados no ambiente selecionado. As suas escolhas são limitadas a ambientes de inicialização que você validou.

1. Clique no botão **Validar licenças** na barra de ferramentas OSD.
2. Na lista **Ambiente de pré-inicialização padrão**, selecione **Linux** ou **Windows** como seu ambiente de pré-inicialização padrão.
3. Clique em **OK**.

Personalização das imagens com o Gerenciador de instalação e Sysprep

É possível usar os utilitários Gerenciador de instalação e o Sysprep da Microsoft ao distribuir imagens do Windows 2003, Windows XP e do Windows XP x64 Edition. O Sysprep personaliza uma instalação Windows de forma que quando o SO reinicializa, ele procura um arquivo de resposta (sysprep.inf) e reconfigura a si mesmo para o novo dispositivo. O Gerenciador de instalação cria o arquivo de resposta sysprep.inf utilizado pelo Sysprep.

Antes de criar scripts de distribuição do SO, você deve executar o Gerenciador de instalação da Microsoft (setupmgr.exe) e criar um arquivo de resposta sysprep.inf para as imagens que estão sendo distribuídas. É possível usar esse arquivo como base para qualquer script de distribuição do SO criado por meio da seleção da opção **Usar arquivo sysprep.inf existente como um modelo** na página **Especificar informações sobre arquivo Sysprep** do assistente. Quaisquer configurações de script de distribuição do SO realizadas no assistente serão substituídas por opções equivalentes no arquivo sysprep.inf de modelo.

Usar o Sysprep em imagens do Windows 2000/XP permite à distribuição do SO consultar o banco de dados núcleo de cada dispositivo que você está distribuindo e migrar determinadas configurações de usuário, como:

- nome do computador no Windows;
- GUID (o identificador exclusivo usado para identificar dispositivos no banco de dados núcleo).

Também é possível definir essas opções globalmente para imagens distribuídas:

- fuso horário;
- chave de licença de volume;

- nome e organização registrados;
- grupo de trabalho/domínio/unidade organizacional LDAP (OU).

A distribuição do SO usa as informações do banco de dados núcleo e do script de distribuição de geração de imagem para criar um sysprep.inf personalizado para cada dispositivo cuja imagem está sendo criada. A distribuição do SO insere o sysprep.inf em cada imagem do dispositivo.

Informações adicionais

Para obter mais informações sobre a Gerenciador de instalação e Sysprep, consulte a documentação sobre os utilitários Gerenciador de instalação e Sysprep no site da Microsoft. O Sysprep tem muitos recursos eficientes a serem usados, além dos que estão no escopo deste documento.

Você pode também encontrar ajuda para problema com o uso do Sysprep no site da Comunidade de suporte da LANDesk; visite community.landesk.com.

Criar uma imagem do sysprep

1. No dispositivo cuja imagem será capturada, faça as alterações na configuração ou personalização para prepará-lo para criar uma imagem.
2. Na raiz do disco rígido do dispositivo, crie uma pasta c:\sysprep.
3. De um CD de instalação do Windows 2000 ou do Windows XP, abra \Support\Tools\DEPLOY.CAB e copie os arquivos **sysprep.exe** e **setupcl.exe** para a pasta sysprep criada.
4. Abra um prompt de comando do DOS e altere para a pasta sysprep. Execute o Sysprep. Caso a opção de reinicialização não seja usada, será necessário desligar o dispositivo no menu Iniciar depois de aparecer uma mensagem solicitando o desligamento.
5. Reinicie no DOS e execute a ferramenta de criação de geração de imagem manualmente.

Visão geral do Distribuição baseada no PXE

A distribuição do SO oferece suporte à inicialização de PXE e à distribuição de imagem. Com o Distribuição baseada no PXE, você pode inicializar dispositivos habilitados no PXE existentes e novos, bem como executar um script de distribuição do SO no dispositivo em um menu de inicialização DOS PXE personalizado ou analisar dispositivos para o banco de dados núcleo e agendar uma tarefa de distribuição de imagem por meio da ferramenta **Tarefas agendadas**.

A distribuição baseada no PXE é um modo útil de criar imagens de dispositivos em várias situações, tais como:

- Provisionamento inicial de novos dispositivos
- criação de geração de imagem para dispositivos em um laboratório de teste ou treinamento;
- Restauração de imagens de dispositivos corrompidos

O LANDesk Management Suite oferece várias opções de uso do PXE para distribuir imagens do SO:

- Inicialização gerenciada LANDesk, permite que você use dispositivos já estabelecidos para criação de imagem.
- Um menu de inicialização do PXE, permite que você selecione uma opção de dispositivo interativamente
- Uma fila de retenção PXE, que adiciona dispositivos automaticamente à uma fila na inicialização de PXE

Fundamentos do protocolo PXE

O PXE (Preboot Execution Environment, Ambiente de execução de pré-inicialização) é um protocolo de rede padrão da indústria que habilita dispositivos a inicializarem e a criarem imagens da rede, fazendo o download e instalando um arquivo de imagem executável de um servidor de imagem, antes de o dispositivo realizar a inicialização do disco rígido local. Em um dispositivo habilitado no PXE, o protocolo PXE é carregado da memória de reprogramação do adaptador da rede ou do ROM ou do BIOS do sistema.

O PXE usa os seguintes padrões de comunicação:

- DHCP (Dynamic Host Configuration Protocol)
- TFTP (Trivial File Transfer Protocol)
- MTFTP (Multicast Trivial File Transfer Protocol)

Quando um dispositivo habilitado no PXE realiza a inicialização, envia uma solicitação de descoberta do DHCP. Se for localizado um servidor DHCP que implementa PXE, o servidor atribuirá um endereço IP ao dispositivo e enviará informações sobre servidores de inicialização PXE disponíveis. Depois de concluir o processo de descoberta do DHCP, o dispositivo contata o servidor PXE e faz o download de um arquivo de imagem por meio do TFTP. O script de criação de geração de imagem é executado, carregando a imagem do SO do servidor de criação de geração de imagem no dispositivo. O arquivo de imagem é referido como um script de distribuição do SO.

Para aprender mais sobre o PXE e suas respectivas tecnologias e funcionalidades, leia a PXE Specification v2.1, localizada no site http://download.intel.com/design/archives/wfm/downloads/pxespec.pdf.

Visão geral da configuração do PXE com o Management Suite

A lista a seguir oferece uma visão geral do processo que você deverá concluir para usar a inicialização PXE nos dispositivos que você gerenciar.

1. Certifique-se que o ambiente OSD foi validado para DOS ou Ambiente de imagem do Windows PE. Para verificar, clique em **Configurar > Serviços** e na guia **Geral** clique no botão **Validação de OSD**. A imagem que você usar com a inicialização por PXE precisa corresponder ao SO que você validou.
2. Criar um script de configuração de OSD para capturar uma imagem. Clique em **Ferramentas> Distribuição> Distribuição de SO** e na barra de ferramentas selecione o tipo de PE que você usará. Você deve criar os scripts que quer disponibilizar para os operadores no menu de inicialização do PXE.
3. Adicionar scripts ao menu de inicialização do PXE. Clique em **Ferramentas > Distribuição > Menu de inicialização do PXE**. Arraste scripts da janela de Distribuição de SO para a janela menu de inicialização do PXE e classifique os scripts como você deseja que eles apareçam no menu de inicialização do PXE.
4. Distribua um representante de PXE em cada sub-rede onde você quer disponibilizar a inicialização PXE. Um script de distribuição representante de PXE está localizado na pasta **Todos os outros scripts** (clique em **Ferramentas > Distribuição > Distribuição de SO > Scripts OSD > Todos os outros scripts**).
5. Configure dispositivos habilitados para PXE nas opções de reinicialização que preferir: selecione a reinicialização em rede na hora do boot ou configure o BIOS para que o dispositivo inicialize primeiro a partir da rede.
6. Ao inicializar um dispositivos habilitados para PXE, pressione **F8** para menu de inicialização do PXE. Selecione a opção de inicialização que você deseja aplicar ao dispositivo.

Inicializar dispositivos no menu de inicialização do PXE

Quando um dispositivo habilitado no PXE é inicializado, o que ocorre é o seguinte:

1. O dispositivo habilitado no PXE envia uma consulta aos serviços de PXE sendo executados em um representante PXE na rede.
2. Se ele existir em uma sub-rede, responderá e informará ao dispositivo que continue a inicialização usando o PXE.
3. É iniciada uma sessão de inicialização do PXE no dispositivo e o prompt de inicialização do PXE é exibido. A mensagem de prompt padrão é exibida durante quatro segundos, exibindo "Pressione F8 para visualizar o menu." (É possível modificar essas configurações do prompt de inicialização do PXE na guia **Configurar > Serviços > Distribuição do SO**.)
4. Se a tecla **F8** for pressionada antes do término da contagem regressiva, será exibido um menu de inicialização do PXE preliminar, permitindo a escolha das seguintes opções de inicialização:

    - **Inicialização local:** O dispositivo é inicializado na unidade do disco rígido local. Caso não haja a presença do SO, uma mensagem de erro será exibida.
    - **LANDesk:** O dispositivo é adicionado à tela de rede do console (exibe o endereço MAC do dispositivo), no qual é possível agendar um script de distribuição do SO para executá-lo.
    - **Menu de inicialização do :** o dispositivo exibe o menu de inicialização criado por meio da ferramenta menu de inicialização do PXE e é possível selecionar um script de distribuição do SO para executá-lo.

5. Se a tecla **F8** não for pressionada antes do término da contagem regressiva, o dispositivo usará a opção de inicialização padrão. Essa opção é determinada pelas seguintes condições:

    - Se o dispositivo detectar uma tarefa de criação de geração de imagem agendada para ele no banco de dados núcleo (ou uma tarefa pendente ou que falhou), a opção de inicialização padrão passará a ser uma **Inicialização gerenciada pelo LANDesk**.
    - Se o dispositivo *não* detectar uma tarefa de imagem para si, a opção de inicialização padrão passará a ser uma **Inicialização local**.
    - O menu DOS PXE nunca se tornará a opção de inicialização padrão.

6. o script de distribuição do SO agendado será executado no dispositivo.

Tópicos relacionados

"Configuração do prompt de inicialização do PXE" na página 373

"Uso do Menu de inicialização do PXE" na página 374

Uso de representantes PXE

O software de suporte ao PXE é instalado no servidor núcleo como parte da instalação OSD normal. No entanto, para habilitar o suporte PXE, você deve primeiro configurar os parâmetros PXE, em seguida, é necessário distribuir um representante PXE em cada sub-rede da rede em que deseja que o suporte PXE esteja disponível. Os representantes PXE oferecem a escalabilidade na rede, distribuindo imagens do SO a dispositivos em suas respectivas sub-redes.

Os dispositivos em cada sub-rede utilizam os métodos normais de consulta PXE e transferência de arquivos para se comunicarem com o representante PXE residente, que se comunica-se com o servidor núcleo por meio de serviços da Web (HTTP).

NOTA: Desabilitar outros servidores PXE
Se houver qualquer outro servidor PXE em execução atualmente na rede, será necessário desabilitá-lo para usar o suporte PXE do LANDesk.

Distribuindo representantes PXE

É necessário distribuir um representante de PXE em cada sub-rede onde quiser fornecer suporte para inicialização PXE. O representante PXE é configurado pela execução do script Distribuição de representante PXE no cliente selecionado. Este script pré-definido está disponível na ferramenta **Gerenciar scripts** (clique em **Ferramentas > Distribuição > Distribuição de SO > Scripts de OSD** e clique na pasta **Todos os outros scripts**).

É possível dispor de vários representantes PXE em uma sub-rede para ajudar no equilíbrio de carga. Neste caso, o primeiro representante PXE a responder a uma solicitação do dispositivo será o utilizado para se comunicar com o servidor núcleo.

NOTA: Recomenda-se *não* distribuir um representante PXE no seu servidor núcleo.

Não há requisitos de hardware especiais para o dispositivo selecionado para ser um representante XE, mas é necessário atender aos seguintes requisitos de software:

- **Sistema operacional:** Windows 2000 Professional SP4, Windows XP SP3, Windows Vista SP2, Windows 7, Windows Server 2000 SP4, Windows Server 2003 SP2 ou Windows Server 2008.

  Para o Windows 2000, verifique se o serviço do Microsoft MSI está em execução (por padrão, o XP inclui o MSI). Se você já tiver instalado a última versão do service pack, o serviço do MSI deverá estar em execução. Do contrário, você poderá distribuí-lo ao representante PXE alvo no console seguindo estas etapas: Clique em **Ferramentas > Distribuição > Gerenciar scripts**, selecione a tarefa **Distribuição de serviço MSI** em **Todos os scripts** e clique no botão **Agendar**. Nas janelas **Tarefas agendadas**, arraste os dispositivos alvo para a janela, clique com o botão direito na tarefa **Distribuição de serviço MSI** e selecione **Propriedades**, clique em **Agendar tarefa** e especifique uma hora para agendar a Distribuição de serviço MSI.

- **Agentes LANDesk instalados:** Melhoria do agente de distribuição de softwares e do agente do analisador de inventário. Para obter mais informações, consulte "Configuração de agentes" na página 99.

Atualizar representantes PXE

Atualização de representantes PXE Se modificar as configurações da opção de inicialização do PXE (na guia Configurar > Serviços > Distribuição do SO), você precisará atualizar todos os representantes PXE, executando novamente o script Distribuição de representante PXE para efetuar as alterações nos representantes PXE de cada sub-rede. No entanto, a nova execução do script não será necessária se você simplesmente mover os proxies PXE da lista de proxies disponíveis para a lista de proxies Fila de retenção.

Atualizar imagens Windows PE

Ao modificar uma imagem Windows PE de qualquer forma, as mudanças que você fez devem ser transferidas para todos os representantes PXE. Isso é normalmente feito através da redistribuição de representantes PXE, que podem consumir largura da banda e tempo. Para obter mais informações sobre scripts, você pode usar aquela simples cópia da imagem atualizada do Windows PE para atualizar todos os representantes PXE, veja o seguinte documento na Comunidade de usuários da LANDesk:

http://community.landesk.com/support/docs/DOC-7619

Distribuir um representante PXE

É necessário distribuir um representante de PXE em cada sub-rede onde quiser fornecer suporte para inicialização PXE. O representante PXE é configurado pela execução do script Distribuição de representante PXE no cliente selecionado.

Para distribuir um representante PXE:

1. No console, clique em **Ferramentas > Distribuição > Distribuição de SO**.
2. Na janela **Distribuição de sistema operacional**, clique no item de árvore **Todos os outros** . Clique no script **Distribuição de representante PXE** e clique no botão da barra de ferramenta **Agendar**.
3. Na tela de rede do console, selecione o dispositivo alvo nos quais você deseja instalar os serviços PXE.
4. Arraste solte o dispositivo selecionado para a tarefa **Distribuição do representante de PXE** na janela **Tarefas agendadas**.
5. Clique com o botão direito em **Distribuição de representante PXE** clique em **Propriedades** e termine de configurar a tarefa.

Atualizar ou remover representantes PXE

Se você modificar as configurações da opção de inicialização do PXE (na guia **Configurar > Serviços > Distribuição do SO**), você precisará atualizar todos os representantes PXE, executando novamente o script Distribuição de representante PXE para efetuar as alterações nos representantes PXE de cada sub-rede.

O procedimento é similar quando você interrompe o uso de um dispositivo como representante PXE. Execute o script Remoção de representante PXE para remover o dispositivo dos representantes PXE da rede.

Atualizar representantes PXE

1. Clique em **Ferramentas > Distribuição > Distribuição de SO**.
2. Clique em **Todos os outros scripts** e clique em **Distribuição de representantes PXE**. Clique com o botão direito no script e selecione **Agendar**.
3. Arraste e solte os dispositivos alvo na lista tareva adequada na janela **Tarefas agendadas**.
4. Clique com o botão direito na tarefa, clique em **Propriedades**, e termine de configurar a tarefa.

No entanto, a nova execução do script não será necessária se você simplesmente mover os proxies PXE da lista de proxies disponíveis para a lista de proxies Fila de retenção.

Remover representantes PXE

1. Clique em **Ferramentas > Distribuição > Gerenciar scripts**.
2. Clique em **Todos os outros scripts** e clique em **Remoção de representante PXE**. Clique com o botão direito no script e selecione **Agendar**.
3. Arraste e solte os dispositivos alvo na lista tareva adequada na janela **Tarefas agendadas**.
4. Clique com o botão direito na tarefa, clique em **Propriedades**, e termine de configurar a tarefa.

Configuração do prompt de inicialização do PXE

É possível controlar o comportamento do prompt de inicialização do PXE quando os dispositivos tentam realizar a inicialização do PXE.

Quando um dispositivo com PXE habilitado realiza a inicialização, uma solicitação do DHCP tenta iniciar uma sessão do PXE, procurando um servidor (ou proxy) que esteja executando o software de serviços PXE (PXE e MTFTP). Se o dispositivo localizar um servidor PXE, o prompt de inicialização do PXE será exibido no dispositivo durante um tempo especificado em segundos. Ao pressionar a tecla de função F8 durante esta contagem regressiva, é possível acessar o menu de inicialização do PXE e selecionar uma imagem do SO para distribuir no dispositivo.

Para configurar as opções do prompt de inicialização do PXE:

1. Clique em **Configurar > Serviços** e clique na guia **Distribuição de SO**.
2. Insira um valor (em segundos) na opção **Tempo limite**. O valor padrão é 4 segundos. O número máximo de segundos é 60 segundos.
3. Digite uma mensagem na caixa de texto **Mensagem**. A mensagem padrão é “Pressionar F8 para visualizar o menu”. O número máximo de caracteres é 75 caracteres.
4. Clique em **Aplicar** para salvar as alterações ou clique em **OK** para salvar as alterações e fechar a caixa de diálogo.

Se você tem representantes PXE em execução nas sub-redes da sua rede, você deve implementar o prompt de mudanças de inicialização PXE nos proxies atualizando-os. Para fazer isso, agende o script Distribuição de representantes PXE para ser executado em todos os dispositivos que forem representantes PXE.

Uso da inicialização gerenciada pelo LANDesk

A inicialização gerenciada pelo LANDesk é a opção de inicialização padrão quando um dispositivo com o PXE habilitado inicializa e detecta um script de distribuição de imagem que falhou ou um script de tarefa do DOS que falhou para ele no banco de dados núcleo. É possível selecionar também essa opção de inicialização manualmente no dispositivo quando o menu da opção de inicialização é exibido.

Como permite a distribuição autônoma, a inicialização gerenciada pelo LANDesk é útil para dispositivos já estabelecidos para criação de geração de imagem. Por exemplo, você pode preestabelecer novos dispositivos para uma determinada imagem do SO mesmo antes de eles chegarem, importando um arquivo .CSV que contém os endereços MAC do dispositivo para o banco de dados núcleo.

Para preestabelecer dispositivos por meio da opção de inicialização gerenciada pelo LANDesk:

1. Antes de conectar os dispositivos com o PXE habilitado com a rede, adicione suas identificações ao banco de dados núcleo, importando um arquivo .CSV.

2. Agende uma tarefa de distribuição de imagem para os dispositivos. Ocorre a falha da tarefa de criação de geração de imagem porque os dispositivos ainda não estão conectados à rede.
3. Conecte os dispositivos à rede e inicialize-os.
4. Os dispositivos detectarão uma falha na tarefa de criação de geração de imagem e assumirão como padrão a opção de inicialização gerenciada pelo LANDesk.
5. A tarefa de distribuição de imagem que falhou anteriormente será ativada automaticamente e criará a imagem para os dispositivos alvo.

Uso do Menu de inicialização do PXE

O menu de inicialização do PXE permite selecionar de forma interativa um script de distribuição de imagem para um dispositivo sem a necessidade de agendar uma tarefa de distribuição de imagem. Esse método pode ser útil quando há a necessidade de criar novamente a imagem para dispositivos corrompidos. Antes de usar o menu de inicialização do PXE, é necessário configurá-lo primeiro, adicionando os scripts de distribuição do SO que você deseja exibir no menu.

Você cria o sistema do menu de inicialização do PXE, criando diretórios e colocando scripts de distribuição do SO pré-configurados nesses diretórios. A descrição do script será exibida como um item de menu no menu de inicialização do PXE do dispositivo.

Para configurar o menu de inicialização do PXE:

1. Clique em **Ferramentas > Distribuição > Menu de inicialização do PXE**.
2. Para adicionar um novo diretório ou subdiretório ao sistema do menu, clique no botão **Novo** na barra de ferramentas.
3. Digite um nome para o diretório. Por exemplo, o nome do diretório pode descrever a plataforma do SO ou o número de versão das imagens contidas no diretório. Você também pode alterar o nome do diretório sempre que necessário clicando no botão **Renomear** da barra de ferramentas.
4. Clique em **Ferramentas > Distribuição > Distribuição de SO** e, em seguida, arraste e solte os scripts de distribuição de imagem no diretório apropriado na janela **Menu de inicialização do PXE**.
5. Para salvar o menu Inicialização do PXE, clique no botão da barra de ferramentas **Atualizar**.

Você deve clicar no botão **Atualizar** aqui no console se quiser que as alterações apareçam no **menu de inicialização do PXE** em dispositivos PXE ao inicializar.

Os subdiretórios podem se ramificar quatro níveis a partir do diretório superior. Podem ser colocados o máximo de 18 scripts em cada diretório.

Acessar o menu de inicialização do PXE a partir de um dispositivo

1. Inicialize um dispositivo habilitado no PXE.
2. Quando o prompt de inicialização do PXE for exibido, pressione a tecla **F8** antes do término da contagem regressiva.
3. Selecione **Menu DOS PXE**. O sistema do menu configurado na janela Menu de inicialização do PXE do console será exibido.
4. Para abrir um diretório e visualizar seus subdiretórios e imagens, digite o número do diretório e pressione **Enter**. Navegue no sistema do menu e localize a imagem que deseja que seja distribuída no dispositivo. É possível pressionar **B** para voltar um nível ou pressionar **X** para sair do sistema do menu.

5. Para selecionar uma imagem do SO (relacionada a um script de distribuição do SO), digite o número do script e pressione **Enter**. O script será executado, e a imagem será carregada no dispositivo.

Se você sair do sistema do menu sem fazer uma seleção, o dispositivo aguardará uma tarefa de criação de geração de imagem agendada do servidor núcleo.

Tópicos relacionados

"Visão geral do Distribuição baseada no PXE" na página 368

"Uso do Menu de inicialização do PXE" na página 374

Uso da fila de retenção PXE

A fila de retenção PXE é outro método para distribuir remotamente imagens do SO a dispositivos com o PXE habilitado. Esse método é bastante útil nas seguintes situações:

- Em um ambiente de laboratório controlado em que é necessário recriar com freqüência a imagem de todos os dispositivos com uma imagem idêntica.
- Para criar imagens em dispositivos de laboratório que podem, depois, ser transferidos para o ambiente de produção apropriado.

Ao designar um representante PXE da sub-rede como uma fila de retenção PXE, todos os dispositivos com o PXE habilitado da respectiva sub-rede serão automaticamente adicionados à Fila de retenção PXE na tela de rede do console quando inicializarem o PXE. Você também pode adicionar um dispositivo a uma fila de retenção PXE agendando script **PXE – Adicionar à fila de retenção** ao dispositivo, ou copiando o dispositivo diretamente para o grupo da fila de retenção do PXE na tela de rede. Os dispositivos poderão ser agendados para uma tarefa de distribuição de imagem.

Para configurar uma fila de retenção PXE:

1. Configure representantes PXE na rede.
2. Clique em **Configurar > Serviços** e clique na guia **Distribuição de SO**.
3. Selecione e mova os representantes de PXE da lista **Proxies disponíveis** para a lista de **Proxies da fila de espera**.

   A lista de **Proxies disponíveis** mostra todos os representantes PXE disponíveis na rede, identificados pelo nome do dispositivo. Essa lista é gerada pela execução de uma varredura de inventário que detecta o software PXE (protocolos PXE e MTFTP) executados no dispositivo. A varredura de inventário é executada automaticamente sempre que um representante PXE é configurado pela primeira vez.
4. Clique em **Redefinir**.

   O botão Redefinir força todos os dispositivo com o PXE habilitado na mesma sub-rede que o representante PXE selecionado a entrar novamente na fila de retenção PXE na tela de rede do console. Esses dispositivos podem então ser agendados para uma tarefa de criação de geração de imagem. O botão Redefinir será ativado quando você selecionar um representante PXE na lista **Proxies da fila de retenção**.
5. Clique em **OK** para salvar as mudanças e fechar a caixa de diálogo.

Na próxima vez em que um dispositivo da sub-rede realizar a inicialização, ele será adicionado ao objeto Fila de retenção PXE na tela de rede do console.

Distribuir uma imagem a um dispositivo na fila de retenção PXE

1. Clique em **Ferramentas > Distribuição > Distribuição de SO**.
2. Clique em um script de distribuição de SO na lista, em seguida clique no botão **Agendar** da bara de ferramentas.
3. Na tela de rede do console, abra a pasta **Fila de retenção PXE** e, em seguida, selecione os dispositivos alvo para os quais deseja distribuir a imagem.
4. Arraste e solte os dispositivos selecionados na janela **Tarefas agendadas.** Clique com o botão direito na tarefa, clique em **Propriedades**, e termine de configurar a tarefa.

Distribuição baseada no agente

É possível usar o método de distribuição baseada no agente para distribuir imagens do SO para dispositivos que executam o Windows 98, o Windows 2000 ou o Windows XP.

Pré-requisitos

Se o PXE não estiver sendo usado para distribuir imagens, os dispositivos deverão atender aos seguintes critérios:

- estar no banco de dados núcleo se houver imagens de multiprocessadores;
- Inicie o Agente LANDesk padrão e o agente de distribuição de softwares. A distribuição do SO usa o agente de distribuição de softwares para distribuir imagens.

O que ocorre durante uma distribuição baseada no agente

1. O servidor núcleo conecta-se ao dispositivo e executa qualquer comando de pré-configuração especificado no script de distribuição de imagem.
2. A distribuição do SO utiliza o agente da distribuição de software para distribuir um arquivo de partição de inicialização virtual ao dispositivo. Também modifica o setor de inicialização para inicializar neste arquivo, e, em seguida, reinicializa o dispositivo.
3. O dispositivo inicializa no DOS ou no Windows PE (dependendo da sua escolha), detecta e carrega um driver de rede, em seguida, recupera e instala o arquivo de imagem do servidor de imagens.

   Para imagens não-Sysprep, o dispositivo é reinicializado ao término da criação de geração de imagem. A distribuição do SO assume que a tarefa foi concluída após essa reinicialização.

   Para imagens do Sysprep, a distribuição baseada no agente continua desta maneira:

4. Antes de reinicializar e carregar a imagem, o agente do DOS ou do PE Windows substitui o sysprep.inf por um arquivo personalizado do dispositivo.
5. A imagem do cliente é inicializada e se personaliza com base no que está contido no arquivo sysprep.inf.
6. Para as imagens Windows, qualquer comando de imagem posterior especificado no script de distribuição de imagem será executado na chave de registro RunOnce.
7. Para imagens Windows, a distribuição do SO executa o wscfg32.exe usando a configuração de agente do dispositivo padrão para reinstalar os agentes LANDesk.

Uso do Multidifusão dirigida para distribuir scripts

Esta seção abordará a distribuição de imagens por meio da tecnologia Targeted Multicast™ LANDesk®. Multidifusão é mais lenta que a distribuição única. A multidifusão controla a largura de banda e faz o estágio da imagem no disco rígido do dispositivo alvo. No entanto, a multidifusão de quatro ou mais dispositivos geralmente economizará banda larga suficiente para torná-la eficiente.

A Targeted Multicast suporta somente imagens de partição única, mas não imagens de várias partições. Além disso, ao usar a Targeted Multicast com a distribuição do SO, as imagens podem aumentar para 10 arquivos.

Quando ocorre a multidifusão de imagens, o arquivo de imagem faz o cache no dispositivo antes de ser recuperado. O disco rígido do dispositivo deve ter espaço suficiente para o arquivo de imagem e os arquivos recuperados.

Antes de utilizar a multidifusão com a distribuição do SO, verifique se os componentes da multidifusão estão no lugar na sub-rede à qual os arquivos de imagem serão distribuídos. As distribuições de SO de multidifusão podem falhar se não forem especificados representantes de domínio para cada domínio de multidifusão no grupo **Representantes de domínio de multidifusão** da tela de rede. A Multidifusão dirigida requer agentes do LANDesk Management Suite 6.62 ou superior nos dispositivos e um representante de domínio de multidifusão do LANDesk Management Suite 6.62 ou superior na sub-rede.

Se você tentar executar a multidifusão (Multicast) em uma sub-rede que não tenha um representante de domínio de multidifusão, a distribuição iniciará, mas não terminará e será necessário criar um disco de inicialização OSD para inicializar dispositivos manualmente.

Se os roteadores encaminharem difusões direcionadas ao UDP e houver dispositivos do Windows que possam atuar como representantes de domínio de multidifusão na sub-rede na qual a imagem está sendo distribuída, você poderá usar a Targeted Multicast da melhor forma sem designar representantes de domínio de multidifusão.

Se os roteadores não encaminham difusões direcionadas por UDP, selecione manualmente os representantes de domínio de multidifusão para cada sub-rede, verificando se os representantes escolhidos não estão entre os dispositivos para os quais você está fazendo a distribuição. Se você tentar criar uma imagem de qualquer representante de domínio de multidifusão em uma sub-rede, ocorrerá falha na criação da imagem e deixará os dispositivos em um estado que não poderão ser usados.

Especifique quais dispositivos são representantes de domínio de multidifusão

Você pode especificar manualmente os dispositivos que serão representantes de domínio de multidifusão adicionando dispositivos ao grupo **Configuração | Representante de domínio de multidifusão** na tela de rede.

Controlar largura de banda de multidifusão

Você pode controlar a multidifusão mudando as opções no assistente de distribuição de SO. Em um scritp de distribuição de imagem, selecione as opções a seguir:

1. Na página **Métodos e credenciais,** selecione a opção **Download por multidifusão**.
2. Na página **Descoberta de multidifusão**, selecione **Configurar opções avançadas de Multidifusão**.
3. Na página **Opções avançadas**, mude as opções como necessário desejado para reduzir o tráfego na rede.

AVISO: Se o ambiente de multidifusão não for configurado corretamente e a Multidifusão dirigida falhar, pode não ser possível inicializar todos os dispositivos alvo, a menos que as instruções nesta seção sejam seguidas.

Se a Multidifusão dirigida falhar com tarefas de distribuição, pode ser porque o tamanho da unidade máxima de transmissão (MTU) na sua rede está fragmentando os pacotes.

Tópicos relacionados

"Definição do tamanho máximo de pacotes para Multidifusão dirigida com OSD" na página 378

"Criando uma geração da imagem de um disco de inicialização" na página 406

Definição do tamanho máximo de pacotes para Multidifusão dirigida com OSD

Se a Multidifusão dirigida falhar com tarefas de distribuição, pode ser porque o tamanho da unidade máxima de transmissão (MTU) na sua rede está fragmentando os pacotes. O MTU na sua rede determina o tamanho máximo de pacotes. Siga as etapas abaixo para ajustar o MTU utilizado pela multidifusão.

Para definir o tamanho máximo de pacote para 512 bytes para o script da Multidifusão dirigida:

1. Clique em **Ferramentas > Distribuição > Distribuição de SO**.
2. Clique com o botão direito do mouse no script e clique em **Edição avançada**.
3. Adicione a linha a seguir no final da seção do Multicast do script:

   MAX_PACKET_SIZE=512
   Esta string definirá o tamanho máximo de pacote para a Multidifusão dirigida para 512 bytes. O tamanho máximo de pacote pode ser definido entre 256 e 1464 bytes. Uma definição acima desta faixa, ou nenhuma definição, forçará a definição para o padrão de 1464. Uma definição abaixo da faixa forçará a definição para o padrão de 256 bytes.
4. Salve e feche o script.

AVISO: A definição MAX_PACKET_SIZE deve ser pelo menos 28 bytes menor que a Unidade máxima de transmissão (MTU) para a rede em que o pacote estiver sendo distribuído. Isso é determinado pela adição do tamanho do cabeçalho do IP (20 bytes) e do cabeçalho do UDP (8 bytes) que são enviados com cada pacote de dados. A definição do tamanho máximo de pacote mais alto que este limite causará a falha da distribuição.

Exibição de relatórios de status de imagem

Um dispositivo cuja imagem está sendo criada envia atualizações do status ao servidor núcleo. É possível controlar o status na janela Tarefa personalizada ou por meio de um relatório.

Como a distribuição do SO envia comandos de criação de geração de imagem aos dispositivos, os comandos aparecem na janela Tarefa personalizada. Os dispositivos cuja imagem está sendo criada enviam atualizações do status a cada comando de script enviado. Se a distribuição da imagem falhar por alguma razão, será possível saber qual comando falhou.

Razões comuns para a falha na criação de geração de imagem incluem:

- Corrupção da partição.
- Problemas que não podem ser gerenciados pela ferramenta de criação de geração de imagem.

- Autodetecção do adaptador de rede não poder localizar um adaptador de rede;
- Adaptador de rede indetectável especificado não funciona. Se o driver do adaptador de rede especificado falhar ao carregar, o dispositivo ficará travado no prompt do DOS. Será necessário reinicializá-lo manualmente).

A distribuição do SO cria um relatório de status para cada tarefa, mostrando se a tarefa nos dispositivos-alvo foi bem ou malsucedida.

Criação de scripts de criação de geração de imagem

A distribuição de SO do LANDesk fornece as ferramentas de distribuição de SO e de migração de perfil que permitem criar e gerenciar scripts de criação de geração de imagem (distribuição e captura de geração de imagem) e de migração de perfil.

Com a ferramenta de distribuição de SO você pode criar scripts que executam as seguintes tarefas:

- **Capturar imagem:** cria um script que captura e armazena uma imagem do SO de um dispositivo. As imagens podem ser capturadas por meio da ferramenta integrada de geração de imagem da LANDesk ou com uma ferramenta de terceiro, como Ghost, PowerQuest ou outra de sua preferência.
- **Capturar perfil:** cria um script que captura e armazena as configurações exclusivas de usuário, as configurações de aplicativos e do desktop e os arquivos de um dispositivo. É possível usar também essa opção para acessar a caixa de diálogo Gerenciador de coleções para criar um pacote de migração de perfil iniciado pelo usuário que pode ser executado localmente em dispositivos individuais.
- **Distribuir imagem:** cria um script que distribui uma imagem do SO capturada anteriormente para dispositivos alvo.
- **Restaurar perfil:** cria um script que restaura os dados de perfil capturados anteriormente (configurações do usuário, configurações de aplicativos e desktop e arquivos) para dispositivos alvo.
- **Tarefas genéricas do DOS:** cria um script que executa comandos do DOS (inclusive ativações de aplicativos nos dispositivos).

Depois de criado um script, será possível agendá-lo para executar em dispositivos por meio da ferramenta **Tarefas agendadas.**

NOTA: Criação de pacotes de migração de perfil iniciados pelo usuário
Do assistente de Distribuição do SO/Tarefas de migração, é possível acessar também a caixa de diálogo Gerenciador de coleções. Ela permite criar um pacote de migração de perfil iniciado pelo usuário (um arquivo executável de auto-extração) que pode ser distribuído e executado em dispositivos para migração de perfil iniciada pelo usuário. Para obter mais informações, consulte "Migração perfis de usuários" na página 390.

Se você estiver distribuindo uma imagem para dispositivos com o PXE habilitado, será possível adicionar scripts de distribuição de imagem ao menu de inicialização DOS PXE. Esse menu é baseado no DOS e aparece no dispositivo durante uma inicialização PXE.

Administradores (usuários com direito de Administrador do LANDesk) podem copiar scripts para subgrupos de usuários no grupo **Scripts de usuários**.

Notas sobre uso de scripts

- Os nomes de scripts precisam seguir as convenções de nomeação de arquivo do Windows. O assistente usa o nome do script informado como o nome do arquivo. Se forem usados nomes de arquivos não permitidos no Windows, será enviado um erro sobre o uso de caracteres inválidos.

- Todos os scripts são armazenados no servidor núcleo, no diretório \\core\LDMain\Scripts. Se houver vários consoles, os scripts serão exibidos na janela Gerenciar scripts de cada console.
- O assistente recupera as configurações em cada página do último script criado. Se o tipo de script for alterado de uma tarefa de criação de geração de imagem para uma tarefa de migração de perfil ou para uma tarefa do DOS, o assistente limpará as configurações definidas.
- Por causa das mudanças em como as permissões na conta de usuário administrador são tratadas no Windows Vista e especialmente no Windows 7, pode ocorrer que as imagens mestras que você criar que incluirem essas versões do Windows podem não serem distribuídas com sucesso. Nós recomendamos que você visite o site da Comunidade de suporte da LANDesk, community.landesk.com, para ver os documentos com os melhores métodos que descrevem situações de imagem mestra e procedimentos recomendados para criar e distribuir imagens.

Sobre scripts de tarefas do DOS genéricos

- Os scripts do DOS reinicializam os dispositivos alvo selecionados e executam os comandos especificados. Esses comandos remotos são enviados a uma linha por vez.
- Os scripts do DOS são executados na partição de inicialização virtual e passam pelo mesmo processo de detecção de rede da mesma forma que passam as distribuições normais do SO.
- A opção "Abortar esta tarefa se qualquer comando falhar" interromperá a execução se um dos comandos apresentar um código de nível de erro do DOS não-zero. É possível visualizar o status da tarefa do DOS na janela Tarefa personalizada ou por meio de um relatório.

Criar um script de captura de imagem

1. Clique em **Ferramentas > Distribuição > Distribuição de SO.**
2. Na janela **Distribuição do sistema operacional**, clique com o botão da direita em **Todos os scripts OSD** e selecione o tipo de PE você quer usar (por exemplo, selecione Nova configuração de Windows PE).
3. Selecione **Capturar imagem** e clique em **OK**.
4. Aparece um assistente para guiá-lo na criação do script. Preencha cada campo, clicando nos itens no menu da árvore para exibir todos os campos.
5. Para obter ajuda com qualquer um dos campos, clique em **Ajuda**.
6. Quando o script estiver concluído, clique em **Salvar**.

Ao terminar, o script aparece no grupo **Todos os scripts OSD** na janela **Distribuição de sistema operacional**.

Criar um script de distribuição de imagem

1. Clique em **Ferramentas > Distribuição > Distribuição de SO.**
2. Na janela **Distribuição do sistema operacional**, clique com o botão da direita em **Todos os scripts OSD** e selecione o tipo de PE você quer usar (por exemplo, selecione Nova configuração de Windows PE).
3. Selecione **Distribuir imagem** e clique em **OK**.
4. Aparece um assistente para guiá-lo na criação do script. Preencha cada campo, clicando nos itens no menu da árvore para exibir todos os campos.
5. Para obter ajuda com qualquer um dos campos, clique em **Ajuda**.
6. Quando o script estiver concluído, clique em **Salvar**.

Ao terminar, o script aparece no grupo **Todos os scripts OSD** na janela **Distribuição de sistema operacional**.

Modificar scripts de imagem

Você pode modificar scripts sempre que necessário, reabrindo o diálogo de configuração e fazendo as modificações ou mudando o script diretamente no arquivo .ini e modificando qualquer configuração do Sysprep existentes no arquivo .inf associado.

NOTA: Com scripts do DOS, as únicas mudanças que podem ser feitas são entre as linhas REMPINGx=DOS e REMEXECx=reboot.com. As outras linhas do script gerenciam os arquivos de partição de inicialização virtual e o processo de inicialização.

Para modificar um script usando o assistente de configuração:

1. Clique em **Ferramentas > Distribuição > Distribuição de SO**.
2. Clique com o botão direito do mouse no script e clique em **Editar** no menu de atalho (ou clique duas vezes no script).
3. Avance pelo assistente, fazendo as alterações.

Para modificar um scrip ao editar o arquivo .ini

1. Clique em **Ferramentas > Distribuição > Distribuição de SO**.
2. Clique com o botão direito do mouse no script e clique em **Edição avançada**. O arquivo .INI do script abrirá no Bloco de notas. Se houver configurações do Sysprep associadas ao script, o arquivo sysprep.inf também será aberto no Bloco de notas.
3. Faça alterações em um ou em ambos os arquivos.
4. Salve os arquivos.

NOTA: Os arquivos INI são salvos no diretório \\<core>\LDMain\LANDesk\Scripts. Os arquivos INF são salvos no diretório \\<core>\LDMain\LANDesk\Files.

Visão geral da imagem independente de hardware

Ao distribuir imagens para seus dispositivos gerenciados, é difícil manter tantas imagens diferentes baseadas em configurações diferentes de hardware. O novo hardware requer novos drivers e o hardware existente pode ter drivers atualizados que você quer distribuir. Em vez de manter dezenas ou centenas de imagens individuais para várias configurações de hardware, você pode usar a Geração de imagem independente de hardware (HII) para distribuir uma imagem básica para dispositivos diferentes e, em seguida, adicionar os drivers necessários para cada tipo diferente de hardware automaticamente.

A geração de imagem independente de hardware ajuda a resolver os problemas comuns com dispositivos gerenciados. Por exemplo, os arquivos .dll da camada de abstração de hardware (HAL) precisam ser escolhido de forma precisa ou o dispositivo pode reinicializar com uma tela preta após o processo de geração de imagem. Tipicamente os sistemas operacionais não têm a capacidade de reconhecer dispositivos de armazenamento em massa corretamente, portanto é importante ter os drivers corretos ao aplicar a imagem. Além disso, os fabricantes com frequência têm drivers de dispositivo plug-and-play específico ao hardware ou eles criam dependências de driver em seus aplicativos, por isso é possível criar novos problemas ao aplicar a imagem de um dispositivo com o drivers incorretos. Com a ferramenta de geração de imagem independente de hardware do LANDesk Management Suite você pode evitar esses tipos de problemas e obter maior controle do uso de drivers nos seus dispositivos gerenciados.

Você pode usar a geração de imagem independente de hardware do com imagens de qualquer ferramenta de imagens. Você pode definir as imagens com a ferramenta que preferir e, em seguida, criar scripts de geração de imagem no Management Suite que incorpora a ferramenta HII. Se já tiver imagens criadas com outra ferramenta, você pode reusá-las em vez de criar scripts inteiramente novos.

Um descrição simplificada do processo da HII está abaixo. Os detalhes sobre as etapas específicas que você precisará seguir e as considerações para os tipos diferentes de imagens são descritos nas seções seguintes.

1. Quando você distribui uma imagem criada usando a HII, o script de geração de imagem inicializa o dispositivo no ambiente de pré-inicialização do Windows. No ambiente de pré-inicialização, a ferramenta HII selecione o arquivo .dll HAL adequado e o carrega.
2. O SO é instalado no dispositivo mas antes do SO inicializar, o script de geração de imagem da HII determina que drivers são requeridos pelo dispositivo e copia os arquivos de driver para o disco rígido do dispositivo.
3. Os drivers são adicionados ao registro do dispositivo de modo que quando o SO inicializa a configuração do Windows detecta os novo drivers, instala-os e configura o dispositivo com os drivers.
4. Em seguida, o Windows reinicia com os drivers em execução e o agente LANDesk é instalado.

NOTA: Por causa das mudanças em como as permissões na conta de usuário administrador são tratadas no Windows Vista e especialmente no Windows 7, pode ocorrer que as imagens mestras que você criar que incluirem essas versões do Windows podem não serem distribuídas com sucesso. Nós recomendamos que você visite o site da Comunidade de suporte da LANDesk, community.landesk.com, para ver os documentos com os melhores métodos que descrevem situações de imagem mestra e procedimentos recomendados para criar e distribuir imagens.

Configurações da geração de imagem independente de hardware

Para implementar a geração de imagem independente de hardware com scripts de distribuição de SO ou modelos de provisionamento, crie um repositório de drivers que estarão disponíveis à ferramenta de geração imagens. Esses drivers são usados no hardware do qual você deseja gerar a imagem e incluindo drivers de áudio, vídeo, rede, dispositivos de armazenamento em massa e outros tipos de dispositivos.

Armazene os drivers em uma localização em um servidor preferencial e certifique-se que o caminho está acessível através dos métodos UNC e HTTP.

Quando a ferramenta de geração de imagem independente de hardware é executada, ela detecta o fabricante e o modelo do dispositivo e descarrega os drivers associados e os instala no dispositivo durante o processo de geração de imagem.

A criação de um repositório é descrito na seção a seguir. Além disso, existem observações de como incorporar o processo de geração de imagem independente de hardware nos scripts de distribuição de SO e modelos de provisionamento.

Criação de um repositório de driver

Ao planejar e definir as imagens que você quer usar para os dispositivos gerenciados, você terá que decidir quais drivers você quer usar. Para usar esses drivers para a geração de imagem independente de hardware, você cria um repositório de drivers que é gravado em um local (por padrão, no servidor núcleo do Management Suite). Os drivers ficam então disponíveis para qualquer script de distribuição ou provisionamento que quiser executar.

Para criar um repositório, você deve salvar os arquivos do driver em uma pasta. Um arquivo .inf para cada driver deve ser incluído. A ferramenta HII analisa a pasta e cria um arquivo drivers.db3 que é usado para corresponder o hardware do dispositivo com os drivers apropriados.

Para criar um repositório de driver

1. Clique em **Ferramentas > Distribuição > Distribuição de SO**.
2. Clique no botão **Gerenciar biblioteca de driver** na barra de ferramenta.
3. Certifique-se que a localização do repositório está correta. Se arquivos de driver são armazenados em um local diferente, clique em **Procurar** e selecione sua pasta de repositório.
4. Certifique-se que a URL do local do repositório está correta.
5. Clique em **Salvar**.

   A ferramenta de HII analisa a pasta repositório e constrói uma lista de drivers. Após terminar, uma mensagem de êxito indica a contagem do arquivo repositório (o número de arquivos encontrados) e o número de drivers processados (o número de drivers individuais encontrados).
6. Todas as vezes que você adicionar arquivos de driver à pasta de repositório, repita os passos de 1 a 5 para atualizar o arquivo drivers.db3 com os novos dados.

Uso da geração de imagem independente de hardware com scripts de distribuição de SO

Você pode incorporar a geração de imagem independente de hardware no script de distribuição de SO para dispositivos Windows, se o script satisfizer os seguintes requisitos:

- Ele precisa ser baseado no ambiente de inicialização Windows PE
- Ele precisa usar Windows Sysprep para configurar a imagem do SO

Para incorporar a geração de imagem independente de hardware, você precisa selecionar a opção HII no assistente de script para que a ferramenta HII seja executada após o sistema operacional estar instalado.A ferramenta HII seleciona automaticamente o fabricante e o modelo do dispositivo para qual estiver processando a imagem com base nas strings no BIOS do dispositivo.

Para incluir a geração de imagem independente de hardware em um script de distribuição de SO

1. Clique em **Ferramentas > Distribuição > Distribuição de SO**.
2. Em **Scripts OSD**, selecione um script. Clique com o botão direito no script e selecione **Editar**. Ou, para criar um novo script, clique com o botão direito em **Todos os scripts OSD** e selecione **Nova configuração de Windows PE**.
3. Clique em **Métodos e credenciais**. Marque as caixas de seleção **Imagens usam Sysprep** e **Usar a geração de imagem independente de hardware**.
4. Clique em **Opções de Sysprep > Opções de geração de imagem independente de hardware**.
5. Para especificar que somente um UNC é usado para acessar o repositório de HII, marque a caixa de seleção **Uso do UNC para copiar arquivos de drive**.
6. Defina todas as outras opções do script que desejar e clique em **Salvar** para salvar o script.

Uso da geração de imagem independente de hardware com modelos de provisionamento

Você pode incorporar a geração de imagem independente de hardware em um modelo de provisionamento para dispositivos Windows, se o script satisfizer os seguintes requisitos:

- Ele precisa ser baseado no ambiente de inicialização Windows PE
- Ele precisa usar Windows Sysprep para configurar a imagem do SO

Para incorporar a geração de imagem independente de hardware, você precisa adicionar uma opção HII na seção **Instalação pós-SO** do modelo para que a ferramenta HII seja executada após o sistema operacional estar instalado. A ferramenta HII seleciona automaticamente o fabricante e o modelo do dispositivo sendo provisionado, com base nas strings no BIOS do dispositivo.

Para incluir o processo de geração de imagem independente de hardware em um modelo de provisionamento

1. Clique em **Ferramentas > Distribuição > Distribuição de SO**.
2. Sob **Modelos de provisionamento**, selecione um modelo baseado em Windows. Clique com o botão direito no modelo e selecione **Editar**. Ou, para criar um novo modelo, clique no botão **Novo modelo de provisionamento** na barra de ferramentas, dê um nome ao modelo, selecione ambiente do Windows PE e selecione o SO alvo.
3. Clique na **Lista de ações**, em seguida, clique na seção **Instalação pós-SO**.
4. Clique em **Adicionar**. Digite um nome e uma descrição para a ação (como HII) e selecione **Geração de imagem independente de hardware** na lista **Tipo**. Clique em **OK**.
5. Para especificar que somente um UNC é usado para acessar o repositório de HII, marque a caixa de seleção **Uso do UNC para copiar arquivos de drive**.
6. Clique em **Aplicar** para salvar a ação da HII ao modelo e adicione qualquer outras ações ao modelo. Observe que você precisa incluir uma ação de **Reinicialização** na seção **Instalação pós-SO***após* a ação HII.
7. Modifique outras variáveis que quiser, inclusive modelos ou outras configuração para o modelo e clique em **OK** quando tiver terminado.

Visão geral da migração de perfil

Com a migração de perfil para preservar perfis personalizados de usuário, desktops, configurações de aplicativos, conexões de rede, impressoras, arquivos e pastas ao implementar projetos de atualizações ou migração. A migração de perfil oferece suporte a migrações locais de dispositivos individuais, bem como migrações remotas, de grande escala de vários dispositivos na rede.

A ferramenta UMA (User Migration Assistant) é usada para tarefas de migração: é executada em cada dispositivo gerenciado para capturar perfis e restaurá-los em um novo SO. Quando você agenda um script de distribuição de SO, a UMA é instalada no dispositivo gerenciado após a primeira vez que a tarefa "Capturar perfil" ou "Restaurar perfil" é executado no dispositivo. Você também pode executar a UMA como ferramenta independente em dispositivos gerenciados após ser instalado.

Migração de perfil é um processo de duas partes:

1. *Capturando* um perfil exclusivo do dispositivo de origem, consistindo em contas de usuário, configurações de desktop (PC), configurações de rede, impressoras e arquivos de dados e pastas.
2. *Restaurando* o perfil para um dispositivo alvo.

Como funciona a migração de perfil

Usando a migração de perfil, você pode criar scripts separados de captura e restauração. Cada script pode ser agendado para ser executado remotamente em um ou vários dispositivos alvo na rede. O processo de capturar e restaurar perfis é realizado pela ferramenta UMA (User Migration Assistant), um executável que é instalado silenciosamente no dispositivo gerenciado quando o script é executado.

Os itens capturados são relacionados na fonte do arquivo de comando do User Migration Assistant command, um arquivo XML. Cada item no arquivo pode ser ativado ou desativado configurando-s como Verdadeiro ou Falso. Por exemplo, o parâmetro `<mouse>true</mouse>` significa que a configuração do mouse do usuário será capturada. Um exemplo de aquivo de comando é fornecido para a sua referência na pasta <core server>\ldlogon\uma\commandxml.

Pré-requisitos

Para executar uma migração de perfil, os dispositivos devem atender aos seguintes pré-requisitos:

- Os dispositivos devem ser analisados no banco de dados núcleo.
- Os dispositivos devem ter o agente LANDesk padrão, que inclui a análise de inventário, o agendador local e os agentes de distribuição de software. A migração de perfil usa o agente de distribuição de softwares para distribuir arquivos.

Caminhos de migração

A migração de perfil oferece suporte à migração para as seguintes versões do sistema operacional Windows:

- Windows 2000 Professional
- Windows XP Home
- Windows XP Tablet PC Edition 2005
- Windows XP Professional
- Windows Vista Home Basic 32-bit
- Windows Vista Home Premium 32-bit

- Windows Vista Business 32-bit
- Windows Vista Ultimate 32-bit
- Windows Vista Home Basic 64-bit
- Windows Vista Home Premium 64-bit
- Windows Vista Business 64-bit
- Windows Vista Ultimate 64-bit
- Windows 7 Home Premium 32-bit
- Windows 7 Professional 32-bit
- Windows 7 Ultimate 32-bit
- Windows 7 Home Premium 64-bit
- Windows 7 Professional 64-bit
- Windows 7 Ultimate 64-bit

Ambientes de trabalho de um SO de 32 bits pode ser migrado para um SO de 64 bits, mas você não pode migrar de um SO de 64 bits para um SO de 32 bits. Os dispositivos de origem e alvo precisam ser executados em versões do Windows com o mesmo idioma.

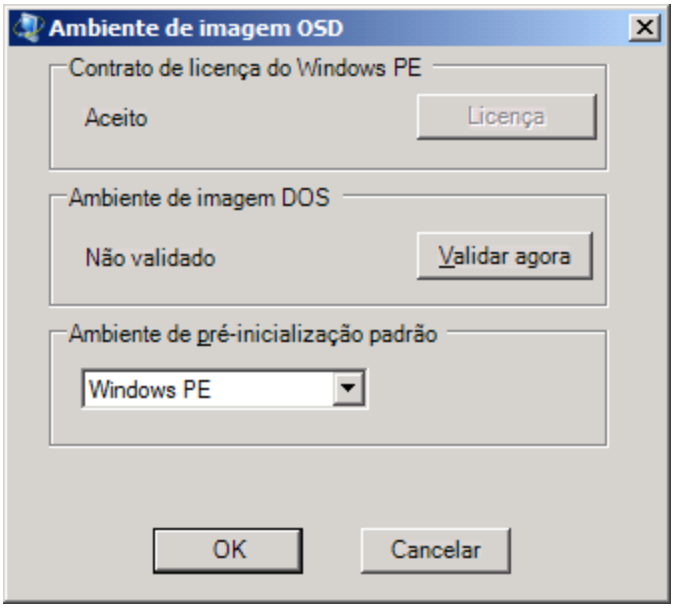
Para ver uma lista detalhada de situações de migração permitidas, consulte "Uso da migração de perfil no LANDesk Management Suite 9", que está disponível para download na comunidade de suporte LANDesk em community.landesk.com.

Criar scripts de migração de perfil

Use o assistente de distribuição de SO para criar scripts que capturam e restauram perfis de dispositivos. Você pode usar o DOS ou o Windows PE para criar scripts de migração de perfil.

Pré-requisitos

Antes de criar scripts de migração de perfil, você deve validar as licenças do ambiente de pré-inicialização do sistema operacional (PE) para DOS PE e Windows PE. Para fazer isso, clique no botão **Validar licenças** na barra de ferramentas da distribuição de softwares SO.



Para o DOS PE, a validação da licença requer um CD de servidor do Windows NT 4 CD e um CD do Windows 98.

Para o Windows PE, você precisa aceitar a licença do ambiente Windows PE instalada com este produto.

Armazenando dados de perfil de vários dispositivos (e vários usuários)

Os dados de perfil são armazenados em arquivos de Assistente de migração do sistema (.sma) em uma estrutura de diretório localizada no caminho UNC que você especificar. Se um script de captura de perfil for executado em vários dispositivos, cada um dos dados de perfil do dispositivo será armazenado em um diretório separado com o mesmo nome exclusivo do computador do Windows.

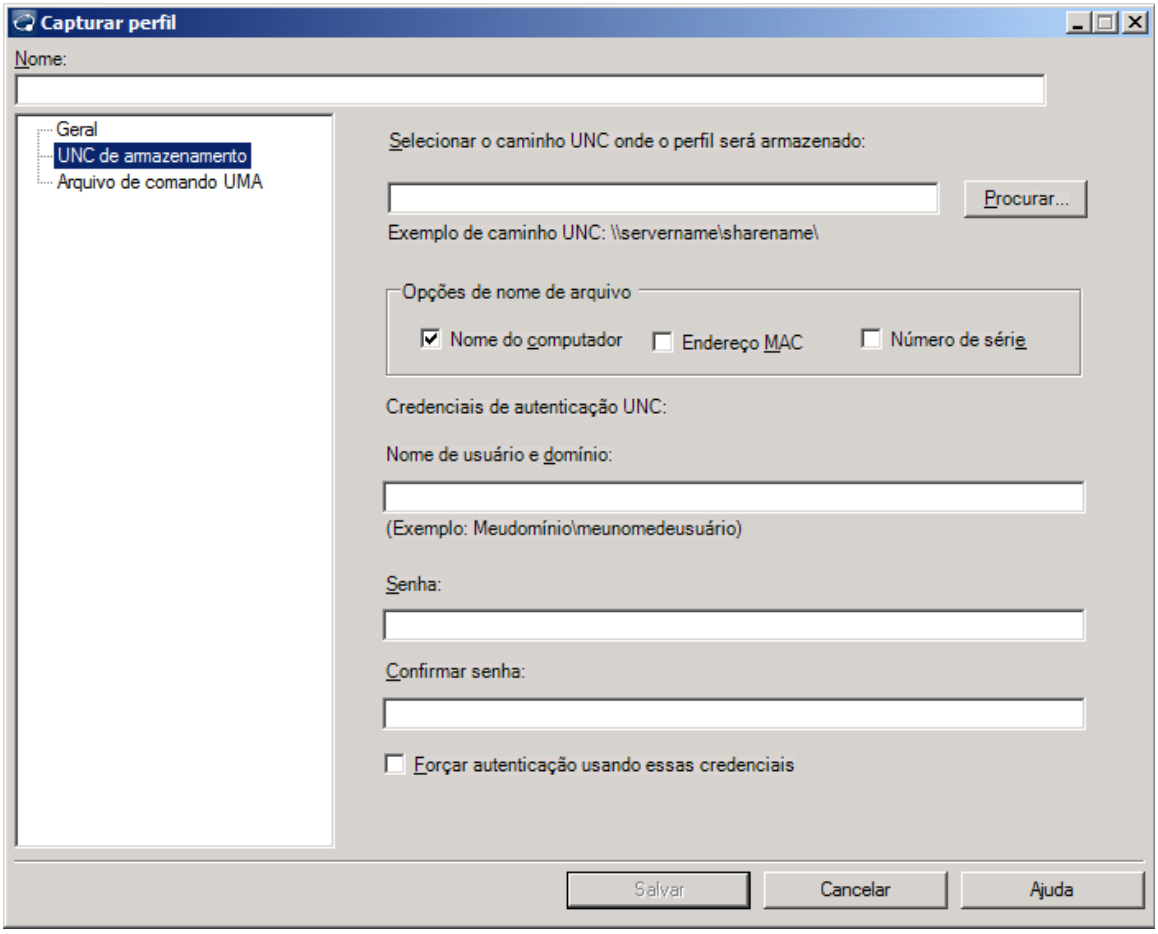
Da mesma maneira, se vários usuários forem localizados e capturados no mesmo dispositivo de origem, cada um dos dados de perfil de usuário será armazenado em um subdiretório separado do diretório do dispositivo e é nomeado com o nome de login do usuário. Em outras palavras, cada dispositivo migrado tem seu próprio diretório de armazenamento de perfil e contém um subdiretório para cada conta de usuário capturada no respectivo dispositivo.

Arquivo de log de migração de perfil

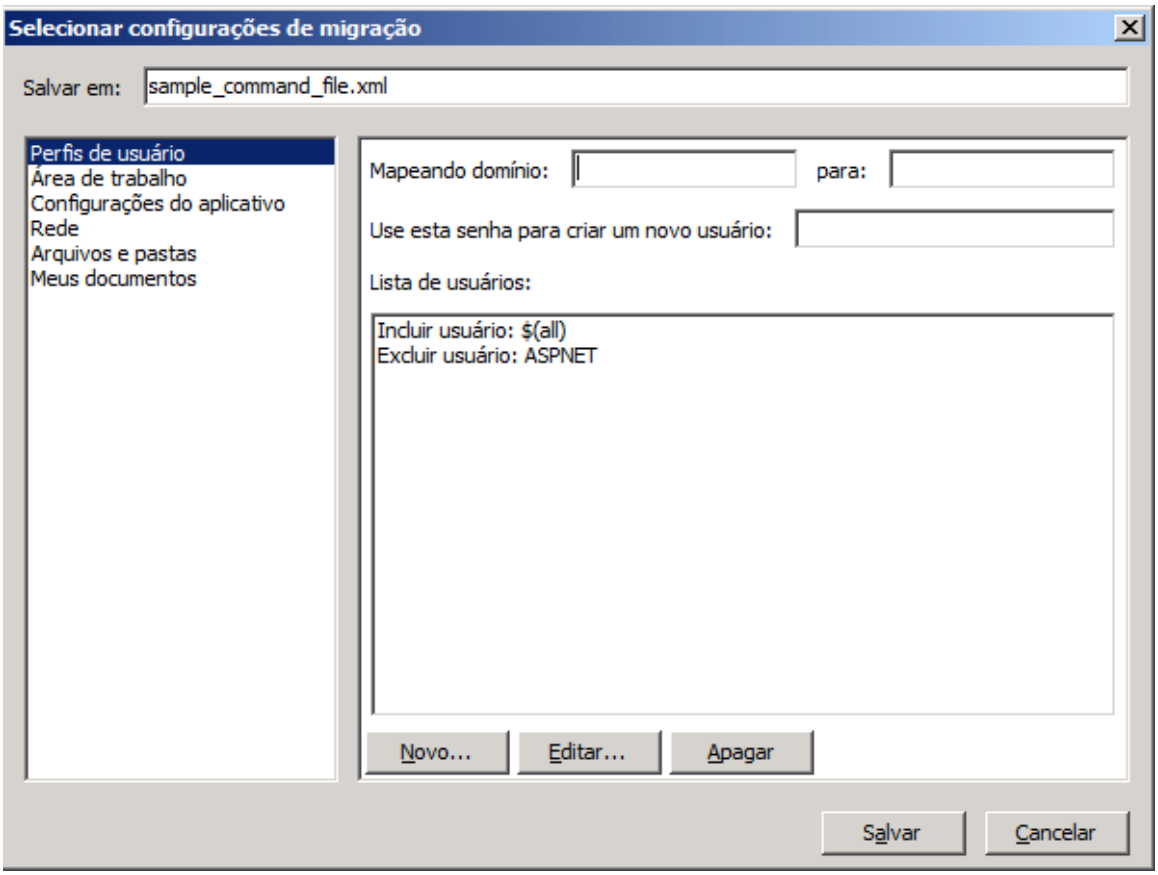
A migração de perfil criar um arquivo de log para cada script que você executar. Os arquivos de log são salvos no servidor núcleo na pasta <servidor núcleo>\ldlog folder. Arquivos de log são nomeados `CJ-OSD-`*`scriptname-date-time`*`.log`

Criar um script de captura de perfil

1. Clique em **Ferramentas > Distribuição > Distribuição de SO**.
2. Na janela **Distribuição de sistemas operacionais**, clique em **Meus scripts OSD** ou **Todos os scripts OSD**.
3. Clique no botão da barra de ferramentas para o PE que você quer usar (**Nova configuração DOS PE** ou **Novas configurações Windows PE**).
4. Selecione **Capturar perfil** e clique em **OK**.
5. Na página **Geral**, digite um nome e uma descrição para o script. Se você quiser que a captura de perfil continue mesmo quando houver erros, selecione a caixa de seleção **Continuar com erros de captura de arquivo**. (Se você selecionar esta opção, os erros são registrados em um arquivo de log.)
6. Na página **UNC do armazenamento**, digite um caminho UNC e as credenciais de autenticação do local no qual deseja armazenar os dados de perfil.
    - Especifique um nome de arquivo padrão para armazenamento de dados de perfil. Use qualquer combinação de nome de computador, endereço MAC e número d série para criar o nome do arquivo de perfil. Por exemplo, se você selecionar **Número de série** e o número de série da máquina é 12345678, o nome do perfil será salvo como "12345678.sma."
    - Marque a caixa de seleção **Foçar a autenticação usando essas credenciais** se você quiser forçar uma autenticação em dispositivos que estão agendados para uma migração de perfil se as credenciais do usuário atualmente conectado falharem.



7. Na página **Arquivo de comando UMA**, especifique o nome e o local do arquivo de comando para ser usado para migração de perfil. Clique em **Editar** para criar um arquivo de comando novo ou editar um existente.
    - Na caixa de diálogo **Configurações de migração**, selecione um arquivo de comando existente e clique em **Editar** ou clique em **Novo** para criar um novo arquivo de comando.
    - Clique em **Perfis de usuários** e adicione os perfis de usuários que você deseja capturar na migração.
    - Clique em **Área de trabalho** e selecione a caixa de seleção para cada item que quiser capturar na migração.
    - Clique em **Configurações de aplicativo** e selecione a caixa de seleção para cada aplicativo que quiser capturar na migração.
    - Clique em **Rede** e selecione a caixa de seleção para cada configuração de rede, unidade e computador que quiser capturar na migração.
    - Clique em **Arquivos e pastas** e adicione os arquivos e pastas que você deseja capturar na migração.
    - Clique em **Meus documentos** e edite as regras de migração da pasta Meus documentos, que são as mesmas das regras de Arquivos e pastas.
    - Clique em **Salvar** para salvar as configurações no arquivo de comando que especificou.



8. Clique em **Salvar** para criar o script de captura de perfil.

Criar um script de recuperação de perfil

1. Clique em **Ferramentas > Distribuição > Distribuição de SO**.
2. Na janela **Distribuição de sistemas operacionais**, clique em **Meus scripts OSD** ou **Todos os scripts OSD**.
3. Clique no botão da barra de ferramentas para o PE que você quer usar (**Nova configuração DOS PE** ou **Novas configurações Windows PE**).
4. Selecione **Restaurar perfil** e clique em **OK**.
5. Na página **Geral**, digite um nome e uma descrição para o script.
6. Na página **Armazenamento do perfil**, digite um caminho UNC e as credenciais de autenticação do local no qual os dados de perfil são armazenados. Você pode especificar a pasta onde o perfil é armazenado, ou escolher a opção **Selecionar o arquivo de perfil** e ir até o arquivo desejado.
    - Especifique um nome de arquivo padrão para armazenamento de dados de perfil. Use qualquer combinação de nome do computador, endereço MAC e número de série para o nome de perfil de arquivo. (Por exemplo, se você selecionar **Número de série** e o número de série da máquina é 12345678, o nome do perfil é "12345678.sma.")
7. Clique em **Salvar** para criar o script de restauração de perfil.

Executar um script de migração de perfil

1. Clique em **Ferramentas > Distribuição > Distribuição de SO**.
2. Na pasta **Todos os scripts OSD**, selecione o script de captura ou de restauração.
3. Clique no botão **Agendar** na barra de ferramentas.
4. Com a ferramenta **Tarefas agendadas**, agende o script para ser executado em um ou mais dispositivos alvo na rede.

Personalização de configurações de migração de perfil

O Assistente de migração do usuário (UMA) armazena informações sobre o conteúdo do perfil que você quer migrar em um arquivo XML denominado *arquivo de comando*. Para especificar que opções são armazenadas quando captura um arquivo, você edita o arquivo de comando.

A maneira mais fácil de criar um novo arquivo de comando é criar um manuscrito de captura de perfil na ferramenta de disposição de Sistema operacional. O arquivo de comando que você cria aqui terá as configurações padrão além das mudanças que fizer nas configurações da área de trabalho, no aplicativo e na rede que foram relacionadas.

Se quiser personalizar ainda mais as muitas configurações no arquivo de comando, você pode criar um novo arquivo XML com as configurações que quiser. Um exemplo de aquivo de comando (sample_command_ file.xml) é encontrado no servidor núcleo na pasta <core server>\ldlogon\uma\commandxml. Copie este arquivo de exemplo para criar arquivos personalizado para tarefas de migração de perfil diferentes.

As seguintes seções contêm ajuda específica para a personalização de um arquivo de comando através da edição do documento XML.

NOTA: Se você excluir um arquivo de comando do servidor núcleo, qualquer script de migração que fizer referência a esse arquivo de comando não executará adequadamente. Você deve também excluir quaisquer scripts que façam referência a outro arquivo de comando.

Migração perfis de usuários

Em uma migração de perfil com script, todas as contas de usuários locais e de domínio localizadas nos disposições de origem são capturadas por padrão *exceto* no caso das contas Todos os usuários e Usuário padrão.

Todas as contas de usuários capturadas serão recuperadas para os dispositivos alvo. Uma conta de usuário que ainda não existe no dispositivo alvo será criada como uma nova conta de usuário local, e suas configurações serão migradas. Antes de recuperar contas de usuários, digite uma senha padrão para essas novas contas de usuários locais. Se uma conta de usuário duplicada já existir no dispositivo alvo, as configurações da conta do usuário capturada (origem) serão migradas para a conta do usuário existente, mas a senha atual do usuário será preservada e deverá ser usada para iniciar a sessão.

Para especificar que perfis de usuários migrar

No arquivo de comando UMA, inclua os nomes de usuário para migrar, na seção `<IncUsers>`. Você pode incluir todos os usuários com a variável `$(all)` ou especificar nomes individuais inclusos em tags `<UserName></UserName>`. Um exemplo de código é mostrado abaixo.

```
<IncUsers>
<UserName>$(all)</UserName>
</IncUsers>
```

Para especificar que perfis de usuários excluir da migração

Exclua os nomes de usuário para migrar na seção `<ExcUsers>` do arquivo de comando UMA. Especifique nomes individuais inclusos em tags `<UserName></UserName>`. Um exemplo de código é mostrado abaixo.

```
<ExcUsers>
<UserName>ASPNET</UserName>
</ExcUsers>
```

Migração de configurações de área de trabalho

Muitas das configurações personalizadas e otimizadas nas áreas de trabalho dos dispositivos podem ser migradas. Essas configurações são definidas na seção `<Desktop>` do arquivo de comando. Para cada item que você quiser incluir, especifique `true` dentro das tags (por exemplo, `<colors>true</colors>` capturará as configurações de cor). Para itens que você não quer incluir, especifique `false` dentro das tags. É possível selecionar dentre as seguintes configurações:

- **Configurações da área de trabalho:** Tema da área de trabalho, esquema de cor, efeitos visuais
- **Acessibilidade:** Configurações de acessibilidade como aquelas para teclado, som e mouse (consulte o Centro de acesso fácil no Painel de controle do Windows Vista o do Windows 7)
- **Active Desktop:** O estado ativo só é suportado no sistema operacional Windows 2000
- **Cores:** Cores da área de trabalho e de janela
- **Ícones da área de trabalho:** Todo o conteúdo da desktop, inclusive pastas, arquivos, atalhos, ícones e posições de ícones
- **Exibir:** Largura, altura e profundidade de cor da área de trabalho
- **Fonte do ícone:** A fonte usada para os ícones da área de trabalho
- **Teclado:** Taxa de repetição do teclado, taxa de intermitência do cursor e demora
- **Mouse:** Configurações de mão esquerda ou direita do mouse, velocidade e taxa de clique duplo
- **Padrão:** O padrão usado para a área de trabalho só é suportado no sistema operacional Windows 2000
- **Proteção de tela:** Configurações da proteção de tela atual
- **Enviar para menu:** Configurações de enviar para menu:
- **Shell:** Para exibir a ordem de classificação de tela, tipo de tela (ícone grande ou pequeno), barra de status e status mostrar/ocultar da barra de ferramentas.
- **Som:** Configurações de som
- **Menu Iniciar:** Comandos do menu Iniciar:
- **Barra de tarefas:** Borda de encaixe, tamanho, sempre na frente, oculta automaticamente, mostrar relógio, mostrar ícones pequenos no menu Iniciar
- **Fuso horário:** Fuso horário do sistema
- **Papel de parede:** Papel de parede da área de trabalho
- **Métricas do Windows:** Espaçamento e organização de janelas minimizadas, fonte da mensagem do diálogo, tamanho do menu e tamanhos da barra de rolagem

As seguintes restrições se aplicam à configurações de área de trabalho:

- **Active Desktop:** Para migrar o Active desktop, inclusive o papel de parede, você precisa selecionar a configuração do papel de parede também.
- **Ícones:** 1) Os espaçamentos vertical e horizontal entre os ícones da desktop não migram de forma precisa. 2) Somente os ícones que estão no diretório Desktop do usuário atual são migrados.

- **Shell:** Para migrar as configurações de shell do Windows Explorer é necessário migrar as configurações de desktop de shell e as configurações de aplicativo do seu Microsoft Internet Explorer. Se o computador alvo usar Windows 2000 Professional, Windows XP, Windows Vista ou Windows 7, as configurações de tela da pasta (como ícones grandes, quadros e detalhes) não migram.
- **Som:** O UMA migra o esquema de som ativo do computador de origem para o computador alvo. O esquema de som é configurado na janela Propriedades de som e multimídia do painel de controle do Windows. Se o esquema de som no computador de origem estiver configurado como Sem som, os sons não serão migrados para o computador alvo. Se o computador de origem usar sons personalizados, é necessário migrar os arquivos de som junto com o esquema de som.
- **Papel de parede:** Se o papel de parede que você deseja migrar for um arquivo JPEG, é necessário também capturar a configuração da Desktop ativa. Não é necessário captura a configuração da Deskto ativa para migrar o papel de parede em formato BMP.

Um exemplo de código de configurações de desktop é mostrado abaixo.

```
<Desktop>
<desktop_settings>true</desktop_settings>
<accessibility>true</accessibility>
<active_desktop>true</active_desktop>
<colors>true</colors>
<desktop_icons>true</desktop_icons>
<display>false</display>
<icon_metrics>false</icon_metrics>
<keyboard>true</keyboard>
<mouse>true</mouse>
<pattern>false</pattern>
<screen_saver>true</screen_saver>
<sendto_menu>false</sendto_menu>
<shell>false</shell>
<sound>true</sound>
<start_menu>false</start_menu>
<taskbar>false</taskbar>
<time_zone>true</time_zone>
<wallpaper>true</wallpaper>
<window_metrics>false</window_metrics>
</Desktop>
```

Migração de configurações de aplicativos e arquivos associados

As configurações persistentes de aplicativos e arquivos associados podem ser migradas como parte de um perfil do dispositivo. Os programas de aplicativos em si *não* são migrados durante a migração de perfil (no entanto, eles podem fazer parte de uma distribuição de imagem do SO).

Aplicativos individuais são especificados para migração na seção `<Applications>` do arquivo de comando. Você pode especificar que todas as configuração são migradas com o uso da variável `$(all)`.

O UMA pode capturar as configurações e personalizações do usuário. Para Lotus Notes e Microsoft Outlook, as configurações podem ser o catálogo de endereço e qualquer e-mail armazenado localmente. Para o Internet Explorer e o Netscape Navigator, as personalizações podem incluir marcadores, cookies e preferências.

Um exemplo de código de configurações de aplicativo é mostrado abaixo.

```
<Applications>
<Application>$(all)</Application>
</Applications>
<Inclusions>
<IncDescription>
<Description>%Personal Directory%\ /s</Description>
```

```
<DateCompare>
<Operand />
<Date />
</DateCompare>
<SizeCompare>
<Operand />
<Size />
</SizeCompare>
<Dest />
<Operation />
</IncDescription>
</Inclusions>
<Exclusions>
<ExcDescription>
<Description>%Personal Directory%\*.vol /s</Description>
<DateCompare>
<Operand />
<Date />
</DateCompare>
<SizeCompare>
<Operand />
<Size />
</SizeCompare>
</ExcDescription>
</Exclusions>
```

Migração de configurações de impressora

As configurações de impressora para migrar são especificadas na seção <Printers> do arquivo de comando. Você pode especificar configurações de impressora individuais colocando o nome da impressora dentro das tags <Printer></Printer> ou pode migrar todas as configurações usando a variável $(all).

NOTA: Só é possível migrar configurações de impressoras que têm definições de impressora integradas no sistema operacional que estiver usando.

Configurações de impressoras virtuais (por exemplo, as configurações para uma impressora XPS) não podem ser migradas de um computador de origem para um computador alvo.

Um exemplo de código de configurações de impressora é mostrado abaixo.

```
<Printers>
<Printer>$(all)</Printer>
</Printers>
```

Migração de configurações de rede

Você pode migrar conexões e configurações de rede, identificação e unidade mapeadas. Essas configurações são definidas na seção `<Network>` do arquivo de comando. Para cada item que você quiser incluir, especifique `true` dentro das tags (por exemplo, `<computer_name>true</computer_name>` capturará o nome do computador). Para itens que você não quer incluir, especifique `false` dentro das tags. É possível selecionar dentre as seguintes configurações:

Configuração de TCP/IP

- IP / Sub-rede / Gateway
- Configuração DNS
- Configuração WINS

Identificação da rede

- Nome do computador
- Descrição do computador
- Domínio / Nome do grupo de trabalho

Outros

- Pastas compartilhadas / Unidades
- Unidades mapeadas
- Rede dial-up
- Rede Microsoft
- Fontes de dados ODBC

As seguintes restrições se aplicam à configurações da área de trabalho:

- **Domínio/Grupo de trabalho** Se o computador de origem for membro de um domínio e você quiser que o computador alvo seja membro do mesmo domínio, crie uma conta para o computador alvo no controlador de domínio. Se o controlador de domínio estiver executando Microsoft Windows 2000 Server, selecione a opção **Permitir computadores pré-Windows 2000 usar esta conta**.
- **Configuração DNS:** As configurações de DNS não migram quando você executar uma migração PC-para-PC.

Um exemplo de código de configurações de rede é mostrado abaixo.

```
<Network>
<ip_subnet_gateway_configuration>false</ip_subnet_gateway_configuration>
<dns_configuration>false</dns_configuration>
<wins_configuration>false</wins_configuration>
<computer_name>false</computer_name>
<computer_description>false</computer_description>
<domain_workgroup>false</domain_workgroup>
<shared_folders_drives>true</shared_folders_drives>
<mapped_drives>true</mapped_drives>
<dialup_networking>true</dialup_networking>
<microsoft_networking>false</microsoft_networking>
<odbc_datasources>false</odbc_datasources>
</Network>
```

Migração de arquivos e pastas

Você pode migrar arquivos individuais ou múltiplos determinados pelo local do diretório e nome do arquivo. As configurações de arquivo e pasta são ativadas na seção `<Applications>` do arquivo de comando. Você pode especificar pastas individuais e arquivos nas seções `<Inclusions>` e `<Exclusions>` do documento para especificar que arquivos você que ou não incluir.

Insira os arquivos que você quer migrar. A página Arquivos / pastas contém os arquivos no computador de origem, classificado por local. Você pode selecionar todos os arquivos em um local ou você pode expandir a árvore e selecionar arquivos individuais.

Considere onde você quer que os arquivos selecionados sejam colocados no computador alvo. Se os discos rígidos nos computadores de origem e alvo forem configurados diferentemente, você precisa selecionar destinos alternativos para arquivos e diretórios.

NOTA: Tenha cuidado ao mudar os locais dos arquivos. Arquivos de lote e configuração podem conter nomes de caminhos totalmente qualificados. Se você mudar os locais dos arquivos e diretórios aos quais os arquivos de lote e configuração se referem, os programas ou tarefas não serão executados corretamente.

Um exemplo de configurações de arquivo e pasta é mostrado abaixo.

```
<FilesAndFolders>
<run>true</run>
</FilesAndFolders>
<ArchiveFile>
<filename></filename>
</ArchiveFile>

<Inclusions>
<IncDescription>
<Description>%Personal Directory% /s</Description>
<DateCompare>
<Operand></Operand>
<Date></Date>
</DateCompare>
<SizeCompare>
<Operand></Operand>
<Size></Size>
</SizeCompare>
<Dest></Dest>
<Operation></Operation>
</IncDescription>
</Inclusions>
<Exclusions>
<ExcDescription>
<Description>%Personal Directory%\*.vol /s</Description>
<DateCompare>
<Operand></Operand>
<Date></Date>
</DateCompare>
<SizeCompare>
<Operand></Operand>
<Size></Size>
</SizeCompare>
</ExcDescription>
</Exclusions>
```

Ajuda do Assistente de distribuição de SO e migração de perfil

Este tópico descreve o assistente de tarefas de distribuição de SO/Migração de perfil.

Ajuda do Assistente de tarefas de distribuição de SO/migração de perfil

O assistente das tarefas de distribuição de SO/Migração de perfil é usado para criar scripts que capturam ou distribuem imagem do SO e capturam ou restauram perfis de usuários. Os scripts podem ser agendados como tarefas nos dispositivos alvo da rede. O assistente pode ser acessado com o botão da barra de ferramentas ou pelos menus de atalho na ferramenta de Distribuição de SO (**Ferramentas > Distribuição > Distribuição de SO**)

NOTA: Todas as páginas do assistente de tarefas de distribuição/migração de SO serão descritas aqui. No entanto, as páginas que você realmente verá ao executar o assistente, depende do tipo de tarefa de criar imagem ou de migração selecionada ao iniciar o assistente.

Escolha um tipo de script.

Para começar, especifique o tipo de script OSD/migração de perfil você deseja criar, com base nas seguintes tarefas:

- **Capturar imagem:** cria um script que captura e armazena uma imagem do SO de um dispositivo. As imagens podem ser capturadas por meio da ferramenta de geração de imagem integrada do LANDesk ou com uma ferramenta de terceiro, como Ghost, PowerQuest ou outra de sua preferência.
- **Capturar perfil:** cria um script que captura e armazena as configurações exclusivas de usuário, as configurações de aplicativos e do desktop e os arquivos de um dispositivo. É possível usar também essa opção para acessar a caixa de diálogo Gerenciador de coleções para criar um pacote de migração de perfil iniciado pelo usuário que pode ser executado localmente em dispositivos individuais.
    - **Continuar com erros de captura de arquivo:** permite ao processo de captura de arquivo continuar mesmo se os arquivos designados para serem capturados reportarem erros de arquivo (por exemplo, nomes de arquivo inválidos ou arquivos que mudam de tamanho durante a captura). A captura de perfil termina e os erros de arquivos são registrados em um arquivo de log.
- **Distribuir imagem:** cria um script que distribui uma imagem do SO capturada anteriormente para dispositivos alvo.
- **Restaurar perfil:** cria um script que restaura os dados de perfil capturados anteriormente (configurações do usuário, configurações de aplicativos e desktop e arquivos para dispositivos alvo).

Novo script de tarefas do DOS genéricas

Este botão da barra de ferramentas cria um script que executa comandos do DOS (inclusive ativações de aplicativos nos dispositivos).

Sobre a página Geral

Use esta página para configurar as seguintes características de uma tarefa de criar imagem do SO:

- **Nome:** identifica o script com um nome exclusivo. Se o nome informado já estiver sendo usado, você receberá um prompt solicitando a substituição do script existente. Insira um nome que ajude a identificar o script por sua função ou pelos dispositivos alvo desejados na rede.
- **Descrição** (opcional): Texto extra que descreve o script.
- **Continuar com erros de captura de arquivo:** permite ao processo de captura de arquivo continuar mesmo se os arquivos designados para serem capturados reportarem erros de arquivo (por exemplo, nomes de arquivo inválidos ou arquivos que mudam de tamanho durante a captura). A captura de perfil termina e os erros de arquivos são registrados em um arquivo de log.

NOTA: Se você adicionar esse script ao Menu DOS PXE do LANDesk, a descrição informada aqui será exibida no menu.

Sobre a página Capturar imagem — Credenciais

Use esta página para fornecer credenciais de autenticação para compartilhamento(s) da rede, onde a imagem do SO e a ferramenta de imagem usadas para criar a imagem são armazenadas.

NOTA: Você pode inserir somente um conjunto de credenciais que será usado para acessar os dois compartilhamentos. Portanto, eles deverão possuir credenciais compatíveis. As credenciais devem pertencer a uma conta de usuário local no dispositivo que hospeda o compartilhamento.

- **Domínio e nome de usuário:** identifica uma conta de usuário com as credenciais necessárias para o usuário iniciar a sessão no compartilhamento da rede.
- **Senha e Confirmar senha:** digite e confirme a senha do usuário.

Sobre a página Capturar imagem — Informações da imagem

Use esta página para especificar o tipo de imagem que você deseja capturar com este script, o local no qual a imagem será armazenada e o local no qual a ferramenta de criação de imagem está localizada.

- **Tipo de imagem:** identifica o tipo de arquivo (formato) da imagem capturada por este script, selecionado na lista de ferramentas de criação de imagem.
- **Inserir o Caminho UNC do diretório:** localiza o servidor e o compartilhamento nos quais o arquivo de imagem será armazenado. A imagem deve ser armazenada em um compartilhamento acessível pelos dispositivos. Observe que o nome do compartilhamento não pode incluir espaços. É possível informar apenas o nome do dispositivo no formato UNC e, em seguida, procurar o caminho restante, clicando no botão Procurar. Em alguns casos a navegação ao caminho insere um caminho local. É necessário converter esse caminho para o formato UNC.

NOTA: Durante o processo de criação de imagem, os dispositivos mapearão este caminho UNC para a unidade I.

- **Inserir o caminho UNC na imagem do aplicativo:** localiza o servidor e o compartilhamento nos quais a ferramenta de criação de imagem (compatível com o tipo de imagem selecionado anteriormente) está localizada, inclusive o nome do arquivo executável da ferramenta. Observe que o nome do compartilhamento não pode incluir espaços. Em alguns casos a navegação ao caminho insere um caminho local. É necessário converter esse caminho para o formato UNC.

NOTA: Durante o processo de criação de imagem, os dispositivos mapearão este caminho UNC para a unidade H.

- **Selecione a partição:** (somente imagens do Windows PE) Permite a escolha da partição no dispositivo gerenciado ao qual você deseja distribuir a imagem. A partição que você selecionou se torna unidade C:

Sobre a página Capturar imagem — Comandos adicionais

Use esta página para personalizar o script adicionando comandos personalizados.

- **Digite comandos adicionais a serem executados antes do dispositivo do usuário ser reinicializado e a imagem criada:** é possível adicionar comandos a esta caixa de texto, um por

linha, como se estivesse digitando em um prompt de comando do DOS. Os comandos são enviados aos dispositivos um de cada vez. Estes comandos são executados após o cliente ser reinicializado e a imagem ser criada:

Sobre a página Distribuir imagem — Métodos e credenciais

Use esta página para fornecer credenciais de autenticação para compartilhamento(s) da rede, onde a imagem do SO e a ferramenta de imagem usadas para criar a imagem são armazenadas.

- **Download por multidifusão:** Usa os representantes de domínio de multidifusão nas sub-redes da rede para distribuir a imagem do SO por meio da tecnologia de Multidifusão dirigida LANDesk. A multidifusão permite a transmissão de pacotes de softwares para vários dispositivos de uma vez, reduzindo bastante os requisitos de tempo e largura de banda. Em vez de enviar um pacote pela rede para cada dispositivo, apenas uma transferência é realizada para cada sub-rede.

NOTA: Antes de usar a multidifusão, verifique se seus componentes de multidifusão estão posicionados na sub-rede na qual a distribuição será executada. A Multidifusão dirigida exige agentes do LANDesk Management Suite 6.62 ou posterior e um representante de domínio de multidifusão LANDesk Management Suite 6.62 ou posterior.

- **Imagem utiliza SysPrep:** indica que o Microsoft Sysprep foi usado para configurar a imagem do SO a ser distribuída. Selecionar esta opção permite especificar opções de distribuição e informações do arquivo Sysprep posteriormente no assistente.
- **Usar imagem independente de hardware:** Selecione esta opção para incluir a ferramenta de imagem independente de hardware no processo de imagens. Esta ferramenta permite definir uma imagem básica que pode ser aplicada a múltiplos modelos de dispositivo e então injeta drivers em cada dispositivo com base no fabricante e modelo. Se você selecionar esta opção, você precisa também especificar as opções do processo de imagem independente de hardware na seção**Opções do Sysprep**.
- **Incluir migração de perfil:** integra os processos de captura e restauração de perfil como parte do trabalho de distribuição de imagem. Selecionar esta opção permite especificar opções de migração de perfil posteriormente no assistente.

NOTA: Você pode inserir somente um conjunto de credenciais que será usado para acessar os dois compartilhamentos. Portanto, eles deverão possuir credenciais compatíveis. As credenciais devem pertencer a uma conta de usuário local no dispositivo que hospeda o compartilhamento.

- **Domínio e nome de usuário:** identifica uma conta de usuário com as credenciais necessárias para o usuário iniciar a sessão no compartilhamento da rede.
- **Senha e Confirmar senha:** digite e confirme a senha do usuário.

Sobre a página Distribuir imagem — Descoberta de multidifusão

Use esta página para configurar as seguintes opções básicas de multidifusão dirigida para um script de distribuição de imagem.

- **Usar o Descobrimento de domínio de multidifusão:** pesquisa representantes de domínio de multidifusão em sub-redes da rede antes de usar a Multidifusão dirigida para distribuir a imagem para dispositivos na rede.

- **Usar Descobrimento de domínio de multidifusão e salvar resultados:** Pesquisa representantes de domínio de multidifusão nas sub-redes da rede antes de distribuir a imagem e salva os dados resultantes para ajudar a facilitar no futuro distribuições de multidifusão dirigida.

NOTA: Apenas um resultado da descoberta é salvo por vez, portanto, selecionar esta opção para um script de distribuição de imagem substituirá os resultados da descoberta anterior.

- **Usar os resultados da última descoberta de domínio de multidifusão:** usa a lista mais recente de representantes de domínio de multidifusão descobertos ao distribuir a imagem para os dispositivos.

  Selecione esta opção *somente* se já tiver salvo os dados resultantes de uma descoberta de representante de domínio de multidifusão pelo menos uma vez.

- **Configurar opções avançadas de Multidifusão:** permite personalizar ainda mais o comportamento da Multidifusão dirigida para um script de distribuição por meio da configuração de opções avançadas de multidifusão na página seguinte do assistente.
- **Representantes de domínio podem ativar dispositivos gerenciados:** Use esta opção se desejar que os computadores que ofereçam suporte à tecnologia Wake On LAN sejam ligados para que possam receber a multidifusão. Você pode usar a caixa de diálogo Opções de multidifusão para configurar o tempo que os representantes de domínio devem aguardar para fazer a multidifusão após o envio do pacote Wake On LAN. O período de espera padrão é de 120 segundos.
- **Número de segundos a esperar Wake on LAN:** Tempo de espera dos representantes de domínio para fazer a multidifusão depois que o pacote Wake On LAN for enviado. O período de espera padrão é de 120 segundos. Se alguns computadores na rede demorarem mais do que 120 segundos para a reinicialização, você deverá aumentar esse valor. O valor máximo permitido é 3600 segundos (uma hora).

Sobre a página Distribuir imagem — Opções avançadas

Use esta página para configurar as seguintes opções avançadas de multidifusão dirigida para um script de distribuição de imagem.

- **Número máximo de Representantes de domínio de Multidifusão trabalhando simultaneamente:** controla o número máximo de representantes de domínio de multidifusão que podem distribuir ativamente uma imagem por meio da Multidifusão dirigida ao mesmo tempo.
- **Número de dias que os arquivos ficam no cache do dispositivo gerenciado:** controla o período durante o qual o arquivo de imagem que está sendo multidifundido pode residir no cache local em cada dispositivo alvo. Após esse período, o arquivo será automaticamente removido.
- **Número de dias que os arquivos ficam no cache do representante de domínio de multidifusão:** controla o período durante o qual o arquivo de imagem que está sendo multidifundido pode permanecer no cache do representante de domínio de multidifusão. Após esse período, o arquivo será automaticamente removido.
- **Porcentagem de largura de banda usada do núcleo ou do servidor preferencial (WAN):** Controla o percentual de largura de banda usada quando o representante de domínio de Multidifusão não está distribuindo um arquivo de um cachê, mas quando o servidor núcleo ou servidor preferencial é usado. É possível usar esse parâmetro para limitar o uso de largura de banda na WAN.
- **Porcentagem de largura de banda usada parceiro-a-parceiro (local):** Controla o percentual de largura de banda disponível usada quando uma difusão seletiva de parceiro-a-parceiro é usada.

Sobre a página Distribuir imagem — Tipo e caminho da imagem

Use esta página para especificar o tipo de imagem que você deseja restaurar com este script, o local no qual a imagem será armazenada e o local no qual a ferramenta de criação de imagem está localizada.

- **Tipo de imagem:** identifica o tipo de arquivo (formato) da imagem existente que você deseja distribuir com este script, selecionado na lista de ferramentas de criação de imagem.
- **Inserir o Caminho UNC do diretório:** localiza o servidor e o compartilhamento nos quais o arquivo de imagem será armazenado, inclusive o nome do arquivo da imagem. A imagem deve ser armazenada em um compartilhamento acessível pelos dispositivos.
- **Inserir o caminho UNC na imagem do aplicativo:** localiza o servidor e o compartilhamento nos quais a ferramenta de criação de imagem (compatível com o tipo de imagem selecionado anteriormente) está localizada, inclusive o nome do arquivo executável da ferramenta.
- **Selecione a partição:** (somente imagens do Windows PE) Permite a escolha da partição no dispositivo gerenciado ao qual você deseja distribuir a imagem. A partição que você selecionou se torna unidade C:

Sobre a pasta Distribuir imagem — Ferramenta comandos adicionais

Adicione comandos Powerquest nesta página se estiver usando Powerquest como ferramenta de criação de imagem. A página é obscurecida se você não selecionou Powerquest como ferramenta de imagem.

Sobre a página Distribuir imagem — Comandos de pré-inicialização

Use esta página para personalizar o script adicionando comandos personalizados.

- **Inserir os comandos a serem executados antes do cliente ser reinicializado e a imagem ser criada:** é possível adicionar comandos a esta caixa de texto, um por linha, como se estivesse digitando em um prompt de comando do DOS. Os comandos são enviados aos dispositivos um de cada vez. Estes comandos são executados antes do dispositivo ser reinicializado e a imagem ser criada.

Sobre a pasta Distribuir imagem — Opções de SysPrep

Use esta página para fornecer as seguintes informações sobre o arquivo Sysprep (Sysprep.inf), usado por este script para modificar a imagem que está sendo distribuída:

- **Selecione um produto do Windows**: Selecione a versão do Windows que você usará no Sysprep.
- **Usar o arquivo SYSPREP.INF existente como modelo:** Usa o arquivo sysprep.inf existente como um modelo para um novo arquivo e indica o local no qual o arquivo existente está armazenado. O novo arquivo Sysprep.inf, contendo as configurações especificadas neste assistente, substitui o arquivo Sysprep padrão existente. Se você desejar que a distribuição do SO baseie o arquivo Sysprep.inf em um já criado, você pode procurar o respectivo arquivo. Se você não selecionar um arquivo Sysprep.inf, a distribuição do SO criará um novo.

NOTA: Após a conclusão do assistente, será possível editar o SYSPREP.INF associado a um script, clicando com o botão direito do mouse no script e em **Edição avançada**.

- **Localização do arquivo Sysprep.inf na imagem sendo distribuída:** Localiza onde o arquivo Sysprep.inf foi armazenado no disco rígido do dispositivo que executou o Sysprep originalmente. (Em

outras palavras, o dispositivo cuja imagem está sendo distribuída por este script.).

- **Configurar opções avançadas do multiprocessador:** Permite a configuração uma imagem para suporte a multiprocessadores.

NOTA: Selecione esta opção somente se a contagem de processadores contida na imagem for diferente da contagem de processadores em qualquer um dos dispositivos alvo.

Sobre a página Distribuir imagem — Multiprocessadores

Use esta página para definir as seguintes configurações de multiprocessadores para a imagem que está sendo distribuída por este script:

- **Selecionar o tipo de sistema operacional para a imagem a ser distribuída:** Especifica o SO que faz parte da imagem sendo distribuída.
- **Especificar o tipo de dispositivo onde a imagem foi criada:** indica se a imagem distribuída foi criada em um dispositivo com um único processador ou com multiprocessadores, com a arquitetura APIC ou MPS.
- **Inserir o local dos arquivos .inf relacionados ao HAL dentro da imagem:** Especifica o caminho para o arquivo .inf relacionado ao HAL da imagem distribuída por este script. O assistente usa os caminhos padrão do arquivo .inf da Microsoft para cada SO. Se os caminhos padrão forem usados durante a configuração do dispositivo para criação da imagem, não mude as informações contidas nesta caixa de texto. Caso contrário, digite o caminho diferente usado no arquivo .inf relacionado ao HAL.

Informações adicionais sobre multiprocessadores

Dispositivos com processador único e com multiprocessadores necessitam de kernel do Windows diferentes. De acordo com a configuração do hardware, pode ser que você consiga usar a imagem de um único processador em um dispositivo com multiprocessadores ou vice-versa.

Os dispositivos que oferecem suporte a recursos de processadores avançados geralmente têm um APIC (Advanced Programmable Interrupt Controller, Controlador de interrupção programável avançado). Esses dispositivos também podem dispor de uma ACPI (Advanced Configuration and Power Interface, Interface de energia e configuração avançada).

a matriz de suporte para compartilhar uma imagem entre dispositivos com um único processador e com multiprocessadores é complexa. Consulte a documentação do Sysprep da Microsoft para obter mais detalhes.

AVISO: Como regra geral ao considerar compartilhar imagens de um único processador e de multiprocessadores, lembre-se de que os dispositivos de origem e destino precisam ter um ACPI APIC HAL ou um não-ACPI APIC HAL. Não é possível usar uma imagem ACPI APIC em um dispositivo não-ACPI APIC ou vice-versa.

Sobre a página Distribuir imagem — Configurações da imagem

Use esta página para especificar as seguintes configurações genéricas para o arquivo Sysprep.inf usado por este script para modificar a imagem que está sendo distribuída:

- **Fuso horário:** indica o fuso horário onde os dispositivos alvo estão localizados.
- **Chave de licença de volume:** especifica o número de licença do SO que será distribuído.

- **Senha do administrador local desta imagem:** fornece a senha do administrador do dispositivo cuja imagem foi criada.
- **Nome:** identifica os dispositivos alvo com um nome, como nome do departamento ou área geográfica.
- **Organização:** Identifica a organização com um nome, como nome da divisão ou empresa.

Sobre a página Distribuir imagem — — Credenciais da rede

Use esta página para especificar as seguintes configurações de rede que você deseja incluir no arquivo Sysprep.inf desta imagem:

- **Grupo de trabalho:** indica que os dispositivos alvo residem em um grupo de trabalho. Se a opção for selecionada, insira o nome do grupo de trabalho na caixa de texto.
- **Domínio:** indica que os dispositivos alvo residem em um domínio. Se a opção for selecionada, insira o nome do domínio na caixa de texto e forneça as seguintes informações da conta de domínio:
  - **Nome de usuário do domínio:** identifica o nome de um usuário no domínio com privilégios para adicionar uma conta de computador ao domínio.
  - **Senha do domínio:** fornece a senha do usuário.
  - **Adicionar dispositivo a uma OU de Active Directory:** permite especificar o caminho (usando a sintaxe do caminho LDAP) para um Microsoft Active Directory OU ao qual você deseja adicionar os dispositivos alvo cuja imagem está sendo criada.
  - **Nome OU:** Insira o nome OU específico.

Sobre a página Distribuir imagem — Convenção de nomes

Use esta página para atribuir a convenção de nomenclatura a dispositivos alvo cuja imagem será criada pelo script de distribuição de imagem.

- **Tentar primeiro obter e usar os nomes dos computadores existentes no banco de dados do Inventário:** preserva os nomes existentes de computadores Windows se os dispositivos alvo já tiverem executado o analisador de inventário. A imagem tentará usar qualquer nome de computador existente no banco de dados núcleo.
- **Quando necessário, use o modelo a seguir para nomear computadores alvo:** fornece um modelo que define uma convenção de nomenclatura para criar nomes exclusivos para dispositivos alvo que não possuem no momento um nome de dispositivo atribuído no banco de dados núcleo. Esse modelo é útil para dispositivos descobertos pelo agente LANDesk e inicializados por PXE. Você pode ver os exemplos na página do assistente.
- **Número inicial:** Digite o número associado com o modelo inserido acima. A distribuição do SO mantém um contador dos números usados. Desta forma, os trabalhos subseqüentes continuam no ponto no qual pararam no último trabalho. Todo o modelo exclusivo tem seu próprio contador. Se o mesmo modelo for sempre usado, o contador estenderá os trabalhos. Clique na caixa de seleção **Sobrescrever valor existente ao salvar** para substituir o número existente com o número inserido em **Número inicial**.

Sobre a página Distribuir imagem — Imagem independente de hardware

Use esta página para configurar o uso da imagem independente de hardware (HII) in a script. A ferramenta de geração de imagem independente de hardware (hiiclient.exe) permite que você use um modelo único de provisionamento ou script de distribuição que pode ser distribuído para múltiplos modelos de dispositivo. É instalada uma imagem básica no dispositivo e a ferramenta HII, então, injeta drivers que são específicos ao modelo de dispositivo.

Esta opção só é usada em imagens baseadas no ambiente de pré-inicialização do Windows. Após o SO ser instalado, mas antes do dispositivo reinicializar, a ferramenta HII detecta o modelo do dispositivo e obtém os drivers para o modelo. Os drivers são instalados no dispositivo e suas informações são incluídas no registro. Após a reinicialização, quando o SO inicia, ele configura os drivers.

- **Usando o UNC para copiar arquivos do driver:** Selecione esta opção se você quer usar somente o endereçamento UNC para acessar o repositório de driver do dispositivo. Se você não selecionar esta opção, o HTTP também pode ser usado para acessar os drivers.

Sobre a página Distribuir imagem — Página do agente LANDesk

Use esta página para fornecer as seguintes informações necessárias para a imagem a fim de instalar o software do dispositivo LANDesk nos dispositivos alvo.

- **Caminho UNC para o diretório que contém o wscfg32.exe:** Especifica o caminho UNC (geralmente \\<nomenúcleo>\LDLogon) para o servidor núcleo ou o centro de serviços em que o wscfg32.exe (o arquivo de instalação do dispositivo LANDesk) reside.
- **Credenciais LANDesk para acessar os servidores núcleo:** Fornece um domínio/nome de usuário, uma senha, e uma senha confirmada para autenticação no servidor núcleo ou no centro de serviços, para que a imagem possa instalar o wscfg32.exe nos dispositivos alvo.

Sobre a página Capturar perfil — UNC de armazenamento

As opções nesta página também são mostradas na página **Armazenamento de perfil** das caixas de diálogo de distribuição de imagem e de restauração de perfil. Use esta página para especificar o local de armazenamento dos dados de perfil e para fornecer credenciais de autenticação.

- **Selecione o UNC a ser restaurado:** (Capturar somente perfil) Especifica o caminho UNC em que os dados de perfil serão armazenados. É possível informar apenas o nome do computador no formato UNC e, em seguida, procurar o caminho restante, clicando no botão Procurar.
- **Selecione a pasta do perfil.** (Restaurar somente perfil) Clique para selecionar a pasta onde o perfil está localizado. Digite o local da pasta ou clique Procurar para achá-lo.
- **Selecione a arquivo do perfil.** (Restaura somente o perfil) Clique para selecionar o perfil. Insira o caminho e o nome do arquivo do perfil ou clique em Procurar para encontrá-lo.

- **Opções do nome do arquivo:** (Capturar perfil) Selecione a opção com a qual você quer salvar o perfil. Você pode selecionar **Nome do computador**, Endereço **MAC**, e/ou **Número de série**. Por exemplo, se você selecionar Número de série e o número de série da máquina é 12345678, o nome do perfil será salvo como "12345678.sma."

  (Restaurar perfil) Selecione a opção que corresponde ao perfil da pasta selecionada. Você pode selecionar **Nome do computador**, Endereço **MAC**, e/ou **Número de série**. Por exemplo, se você escolher endereço MAC e o endereço MAC é 0013207f7da2, o nome do perfile será "0013207f7da2.sma" na pasta do perfile deverá ser usado para restaurar o perfil. Cerifique-se que o arquivo de perfil com o nome correto existe na pasta de perfil selecionada, caso contrário, a tarefa falhará.

- **Domínio e nome de usuário:** identifica um usuário com credenciais de autenticação válidas para o caminho UNC especificado.
- **Senha e Confirmar senha:** especifica a senha do usuário.
- **Forçar a autenticação usando estas credenciais:** Força uma autenticação (fechar e iniciar sessão usando as credenciais especificadas anteriormente) em dispositivos agendados para uma migração de perfil se ocorrer falha no início da sessão atual das credenciais do usuário. Se a falha ocorrer, selecionar esta opção garantirá ao dispositivo direitos suficientes para acessar e salvar dados no compartilhamento da rede no local em que os dados de perfil serão armazenados.

Sobre Capturar perfil — arquivo de comando UMA

Use esta página para especificar o local do arquivo de comando UMA que é usado para capturar perfis de usuário. Este arquivo de comando é um arquivo XML que especifica que elementos incluir no perfil a ser capturado. Esta página permite também editar os elementos mais comuns na arquivo de comando UMA sem abrir o arquivo e editar o código de XML diretamente.

- **Selecionar o arquivo XML de comando do assistente de migração do usuário:** Clique em **Procurar** e selecione o local do arquivo XML.
- **Editar:** Clique neste botão para abrir a caixa de diálogo **Selecione configurações de migração**. Selecione o arquivo de comando UMA que quiser editar e clique no botão **Editar**. Para criar um novo arquivo de comando, clique em **Nova**.
  - **Salvar em:** Especifique o nome do arquivo XML.
  - **Configurações da área de trabalho:** Selecione a caixa de seleção para cada item da desktop que você deseja capturar no perfil.
  - **Configurações do aplicativo:** Selecione a caixa de seleção para cada aplicativo para o qual deseja capturar configurações de usuário no perfil.
  - **Configurações de rede:** Selecione a caixa de seleção para cada configuração de rede e unidade que deseja capturar no perfil.

Para encontrar mais informações sobre a Migração de perfil e o arquivo de comando UMA, consulte "Visão geral da migração de perfil" na página 385"Visão geral da migração de perfil" na página 385

Sobre a página Geral do Editor de script de tarefa DOS

Use esta página para criar um script que executa comandos do DOS (inclusive nomes de aplicativos executáveis) nos dispositivos alvo. Os comandos são enviados aos dispositivos um de cada vez.

- **Nome:** identifica o script com um nome exclusivo. Se o nome informado já estiver sendo usado, você receberá um prompt solicitando a substituição do script existente. Informe um nome que ajude a

identificar de forma fácil e rápida o script por sua função ou pelos dispositivos alvo desejados na rede.

- **Descrição** (opcional): Texto extra que descreve o script.
- **Digite os comandos de DOS a serem executados neste dispositivo:** é possível adicionar comandos do DOS a esta caixa, um por linha, como se você estivesse digitando em um prompt de comandos do DOS. É possível inserir quantos comandos desejar.
- **Abortar este trabalho se qualquer comando falhar:** cancela o trabalho de criação de imagem se qualquer comando do DOS digitado nesta página falhar. Os aplicativos (ativados na linha de comando DOS) que geram um código de nível de erro do DOS quando ocorre falha também fazem com que o trabalho de criar imagem seja abandonado. Se nenhum código de nível de erro for criado quando um comando ou aplicativo falhar, o trabalho de criar imagem continuará.

Validação dos ambientes de inicialização da distribuição do SO

Os ambientes de pré-inicialização de distribuição de SO podem ser usados após você validar a licença para usá-los.

Antes de poder usar os ambientes de inicialização DOS PE, a distribuição de SO deve verificar se você tem uma licença para usar os arquivos necessários ao ambiente de inicialização. A verificação da licença exige o CD do servidor Windows NT 4 e o CD Windows 98.

O Windows PE está instalado para você como parte da instalação do Management Suite. O Kit de ferramentas LANDesk PE usa o software Microsoft Windows Pre-installation Environment (“WinPE”), um produto de terceiros. Para usar o Kit de ferramentas LANDesk® PE, você deve ter aceito o contrato de licença da Microsoft para o WinPE. Clique no botão **Licença** para iniciar.

Acréscimo de drivers à imagem Windows PE

Se houver hardware nos seus dispositivos que não sejam suportados pela imagem padrão Windows PE, é possível adicionar drivers à imagem. Esta caixa de diálogo suporta dois tipos principais de drivers:

- Drivers de armazenamento OEM que incluem um arquivo txtsetup.oem
- Drivers não-OEM que incluem um arquivo .inf

Para adicionar drivers à imagem Windows PE

1. No painel **Distribuição de sistema operacional**, clique no botão **Gerenciar drivers em uma imagem Windows PE** na barra de ferramentas.
2. Procure o arquivo de imagem Windows PE que desejar atualizar.
3. Clique no tipo de driver que estiver instalando e clique em **Avançar**.
4. Clique em **Adicionar** e procure pelo arquivo .inf do driver ou txtsetup.oem e arquivos associados. Clique em **Avançar**.
5. Insira a quantidade de espaço que deseja deixar na imagem Windows PE após redimensioná-la.
6. Clique em **Avançar** ao terminar.

Mudança do papel de parede da imagem Windows PE

Você pode personalizar o papel de parede usado em uma imagem Windows PE.

Para mudar a imagem do papel de parede do Windows PE

1. No painel **Distribuição de sistema operacional**, clique no botão **Trocar o papel de parede da imagem Windows PE** na barra de ferramentas.
2. Selecione se o arquivo da imagem do Windows PE que você quer usar será usando em sistemas operacionais de 32-bit e/ou de 64-bit.
3. Procure o arquivo do papel de parede que deseja usar. Para melhores resultados, use um arquivo bitmap 800x600 de 24 bits.
4. Clique em **OK** ao terminar.

Apêndice: Informações adicionais sobre distribuição do SO e migração de perfil

O capítulo fornece informações complementares sobre os recursos de geração de geração de imagem de SO e migração de perfil de LANDesk.

Este capítulo contém informações sobre:

- "Criando uma geração da imagem de um disco de inicialização" na página 406
- "Adição de distribuições do pacote de aplicativos ao final de um script OSD" na página 407
- "Uso do CSVIMPORT.EXE para importar dados de inventário" na página 407
- "Criação de nomes de computadores personalizados" na página 408
- "Personalização da seção SYSPREP.INF [RunOnce] com valores de inventário indexados" na página 409
- "Uso de imagens em ambientes combinados de processadores individuais e multiprocessadores" na página 409
- "Adição de drivers de adaptador de rede ao ambiente de inicialização DOS" na página 410
- "Adição de drivers de adaptador de rede ao ambiente de inicialização PE Windows" na página 412
- "Uso da ferramenta de geração de imagem do LANDesk para DOS" na página 412
- "Uso da ferramenta de geração de imagem do LANDesk para o Windows" na página 415
- "Compreensão do ambiente de pré-inicialização do Windows PE" na página 418

Criando uma geração da imagem de um disco de inicialização

A distribuição do SO LANDesk (OSD) inclui um utilitário de criação de disco de inicialização que permite criar com facilidade um disco que pode ser usado para inicializar dispositivos em um estado gerenciado na rede da LANDesk. É possível usar esse disco de inicialização para continuar com trabalhos OSD em dispositivos que não tenham um sistema operacional ou cujo trabalho falhou por algum motivo e que não são mais reinicializáveis. Após inicializar um dispositivo por meio do disco de inicialização, será possível agendar um trabalho para ele.

NOTA: O usuário deve ter direitos de administrador no servidor núcleo se quiser criar um disco de inicialização de OSD (mesmo que já tenha o direito OSD).

Os discos de inicialização estão associados ao servidor núcleo no qual foram criados. Se houver vários servidores núcleo, use o disco de inicialização criado no servidor núcleo que você deseja reportar ao dispositivo.

Para criar uma geração da imagem de um disco de inicialização

1. Clique em **Ferramentas > Distribuição > Distribuição de SO**.
2. Na janela **Distribuição do sistema operacional** clique no botão **Criar uma geração da imagem de um disco de inicialização** na barra de ferramentas para abrir a caixa de diálogo Criar geração da imagem de um disco de inicialização.
3. Insira um disquete de 1,44 mb na unidade de disco e verifique se a unidade de disco de destino está correta.

NOTA: Todos os dados no disquete serão apagados.

4. Selecione o adaptador de rede para o qual você deseja que este disquete de inicialização ofereça suporte. O suporte de cada disquete pode ser para apenas um adaptador devido às limitações de espaço no disco.
5. Clique em **Iniciar**. A caixa Status indicará o progresso de criação do disco.
6. Depois de concluído, clique em **Fechar** para sair da caixa de diálogo.

Adição de distribuições do pacote de aplicativos ao final de um script OSD

É fácil tornar a distribuição de um pacote de aplicativos da ESWD parte do script de distribuição do SO.

Para adicionar pacotes ESWD a um script de distribuição do SO:

1. Abra o script do pacote no diretório LANDesk/ManagementSuite/Scripts e copie as linhas de distribuição do pacote REMEXECx=.
2. Edite o script, clicando com o botão direito do mouse nele, na janela Scripts de gerenciamento, e clicando em **Edição avançada**.
3. Cole os comandos ESW REMEXEC na parte inferior do script, alterando a numeração REMEXEC para que os números sejam seqüenciais.
4. Insira uma linha antes das linhas ESWD coladas para LDSLEEP, semelhante ao procedimento a seguir. Isto permite ao SO terminar a inicialização antes de iniciar a instalação do pacote.

   ```
   REMEXECxx=LDSLEEP.EXE 120
   ```

   Substitua xx por um número seqüencial exclusivo.

Uso do CSVIMPORT.EXE para importar dados de inventário

O LANDesk inclui um utilitário de linha de comandos que permite importar dados do inventário para o banco de dados núcleo. Esse procedimento pode ser útil se você estiver instalando novos dispositivos e dispuser de informações como endereços MAC. É possível usar o CSVIMPORT.EXE para importar esses dados para o servidor núcleo, antecipando trabalhos de distribuição do SO para dispositivos alvo.

O CSVIMPORT.EXE necessita de um arquivo de modelo que descreva o conteúdo do campo e em que colunas inserir os dados no banco de dados núcleo. O CSVIMPORT.EXE também necessita do arquivo .CSV que contém os dados compatíveis com o arquivo de modelo especificado. O CSVIMPORT.EXE cria arquivos de minivarredura que podem ser copiados no diretório LANDesk/ManagementSuite/LDScan para que sejam adicionados ao banco de dados núcleo.

Exemplo de arquivo de modelo:

```
Rede - Endereço NIC = %1%
 Rede - TCPIP - Adaptador 0 - Máscara de sub-rede = 255.255.255.0
BIOS - Número de série = %2%
 BIOS - Etiqueta do recurso = %3%
 Exibir nome = %4%
```

Observe que é possível incluir dados personalizados nos arquivos. As entradas %1, %2, etc., referem-se à primeira coluna, segunda coluna e assim por diante. A máscara de sub-rede neste caso será aplicada a todas as entradas, como 255.255.255.0. O arquivo de modelo não poderá apresentar qualquer texto no cabeçalho diferente das informações do modelo real.

Exemplo de arquivo .CSV:

```
0010A4F77BC3, SERIAL11, ASSETTAG-123-1, MACHINE1

0010A4F77BC4, SERIAL21, ASSETTAG-123-2, MACHINE2

0010A4F77BC5, SERIAL31, ASSETTAG-123-3, MACHINE3

0010A4F77BC6, SERIAL41, ASSETTAG-123-4, MACHINE4

0010A4F77BC7, SERIAL51, ASSETTAG-123-5, MACHINE5

0010A4F77BC8, SERIAL61, ASSETTAG-123-6, MACHINE6
```

Execute o CSVIMPORT com estes três parâmetros: <templateFilename> <csvFileName> <outputDirectoryForScanFiles>. Se você quiser que a saída seja inserida imediatamente no banco de dados núcleo, especifique o diretório LANDesk/ManagementSuite/LDScan para ela.

Criação de nomes de computadores personalizados

A página **Convenção de nomes** do assistente de Tarefas de Distribuição do SO/Migração permite criar nomes de computadores com base nos endereços MAC, no texto digitado e nos contadores (nnn...). É possível criar também nomes baseados nos dados de inventário para etiquetas de recursos, números de série e nomes de logon, criando um arquivo COMPUTERNAME.INI.

sintaxe do COMPUTERNAME.INI:

```
[Rename Operations]
tok0=ASSET TAG
tok1=SERIAL NUMBER
tok2=LOGIN NAME
```

Os valores exibidos pelo arquivo .INI substituem o símbolo $MAC na página de convenção de nomenclatura do assistente.

É possível usar apenas os três valores de inventário mencionados anteriormente no arquivo. A distribuição do SO marca as opções na ordem de tok<x>. Nenhum dos três símbolos acima precisa estar no arquivo. A primeira opção tok<x> encontrada que tem um equivalente da entrada do banco de dados substitui o símbolo $MAC para o dispositivo cuja imagem está sendo criada. Por exemplo, no caso anterior, se não houvesse entradas para etiqueta de recurso e número de série no banco de dados, mas houvesse para um nome de logon, o nome de logon seria usado para o símbolo $MAC. Se as opções não forem compatíveis, o endereço MAC será usado para o símbolo $MAC.

A opção de nome de logon exibe o nome de início de sessão localizado pela varredura de inventário mais recente.

Como usar o símbolo do nome do computador nnn

A página **Convenção de nomes** da Distribuição do SO inclui uma opção nnn que substitui um número de 3 a 15 dígitos, de acordo com o número n de caracteres especificado. Para cada modelo de nome de computador usado no assistente, a distribuição do SO mantém um contador dos números usados. Desta forma, os trabalhos subseqüentes continuam no ponto no qual pararam no último trabalho.

Todo o modelo exclusivo tem seu próprio contador. Se o mesmo modelo for sempre usado, o contador estenderá os trabalhos. Se o modelo for alterado depois de distribuir alguns dispositivos e posteriormente o modelo original for usado novamente, o contador indicará o ponto no qual o modelo parou e continuará a contagem.

Personalização da seção SYSPREP.INF [RunOnce] com valores de inventário indexados

O arquivo SYSPREP.INF contém uma seção [RunOnce] que especifica os programas que serão executados após o dispositivo ser inicializado pela primeira vez. Se adicionar seus próprios programas à seção, você pode incluir símbolos do banco de dados na linha de comando do programa se eles forem úteis para o programa que está sendo executado. A distribuição do SO substitui o símbolo especificado pela informação correspondente no banco de dados núcleo.

Exemplos de símbolos:

```
%Computador - Nome de dispositivo%
 %Computador - Nome de logon%
 %Computador - Fabricante%
 %Computador - Modelo%
 %Computador - Tipo%
 %Computador - BIOS - Etiqueta de recurso%
 %Computador - BIOS - Etiqueta de serviço%
 %Rede - TCPIP - Endereço%
 %Sistema - Fabricante%
 %Sistema - Modelo%
 %Sistema - Número de série%
 %Processador - Contagem do processador%
 %Computador - Grupo de trabalho%
 %Computador - Nome de domínio%
```

É possível encadear vários símbolos juntos. Por exemplo, separar dois símbolos por dois-pontos: %Computador - Grupo de trabalho%:%Computador - Nome do dispositivo% pode retornar Meu grupo de trabalho:Meu computador.

NOTA: Você deve usar apenas os símbolos que retornem um único valor.

Uso de imagens em ambientes combinados de processadores individuais e multiprocessadores

Dispositivos com uniprocessadores e multiprocessadores requerem imagens de Windows diferentes. De acordo com a configuração do hardware, pode ser que você consiga usar a imagem de um único processador em um dispositivo com multiprocessadores ou vice-versa.

Os dispositivos que oferecem suporte a recursos de processadores avançados geralmente têm um APIC (Advanced Programmable Interrupt Controller, Controlador de interrupção programável avançado). Esses dispositivos também podem dispor de uma ACPI (Advanced Configuration and Power Interface, Interface de energia e configuração avançada).

a matriz de suporte para compartilhar uma imagem entre dispositivos com um único processador e com multiprocessadores é complexa. Consulte o arquivo UNATTEND.TXT da Microsoft para obter mais detalhes. Geralmente, é necessário lembrar o seguinte em relação ao compartilhamento de imagens de um único processador e de multiprocessadores:

NOTA: os dispositivos de origem e os dispositivos alvo devem ter um ACPI APIC HAL ou um não-ACPI APIC HAL. Não é possível usar uma imagem ACPI APIC em um dispositivo não-ACPI APIC ou vice-versa.

Para configurar informações de vários processadores:

1. Na página **Opções de Sysprep** do assistente de Distribuição de SO/Tarefas de Migração, selecione **Configurar opções avançadas de multiprocessadores**.
2. Na página **Multiprocessadores**, selecione o tipo de imagem de Windows que você está distribuindo.
3. Selecione se a imagem que está sendo criada em um dispositivo **Uniprocessador** ou **Multiprocessador**.
4. Os dispositivos de origem e os clientes alvo têm o mesmo HAL. Se a imagem foi criada em um dispositivo APIC ACPI, selecione **APIC**. Se a imagem foi criada em um dispositivo não-APIC ACPI, selecione **MPS**.

Adição de drivers de adaptador de rede ao ambiente de inicialização DOS

Há três fases de detecção de driver de adaptador de rede que ocorrem durante uma tarefa de distribuição de SO:

Fase 1 (Windows)

O NICINFO.EXE detecta drivers PnP no Windows 2000/XP. Ele também detecta o Windows 9x se for instalado o IE 4.02 ou mais recente. O NICINFO.EXE grava o fornecedor e o ID dos dispositivos DOSNIC.INI detectados na imagem de inicialização virtual.

Fase 2 (DOS)

AUTODETE.EXE procura o DOSNIC.INI deixado pelo NICINFO.EXE e faz a leitura do fornecedor e do ID do dispositivo. AUTODETE.EXE consulta o NIC.TXT para localizar o driver correspondente para carregar. Ele copia o driver de c:\Net\Drivers na imagem de inicialização virtual para a imagem da unidade RAM (r:\Net por padrão). O AUTODETE.EXE em seguida define os arquivos de configuração de pilha da rede DOS da Microsoft, o SYSTEM.INI e o PROTOCOL.INI.

Se o DOSNIC.INI estiver vazio, o AUTODETE.EXE analisará todos os slots do dispositivo PCI, pesquisando os IDs do dispositivo e fornecedor de rede. Se o ID localizado corresponder a uma entrada do NIC.TXT, o AUTODETE.EXE carregará o respectivo driver.

Fase 3 (DOS)

se o DOSNIC.INI estiver vazio e o AUTODETE.EXE não localizar o ID que corresponda ao NIC.TXT, ele carregará o driver especificado no assistente de Distribuição do SO/Tarefas de migração. Se o driver não for carregado, o dispositivo ficará travado no DOS e será necessário reinicializar manualmente. Se nenhum driver foi especificado no assistente, o AUTODETE.EXE salva um arquivo AUTODETE.LOG na raiz da unidade e o dispositivo é inicializado no sistema operacional original.

O NICINFO.EXE e o AUTODETE.EXE não oferecem suporte a adaptadores de rede PCMCIA de 16 bits. Você pode carregar os drivers desses adaptadores de rede, selecionando o driver apropriado no assistente de Distribuição do SO/Tarefas de migração, conforme descrito na Fase 3. NICINFO.EXE pode detectar adaptadores de rede que oferecem suporte a CardBus.

O NICINFO.EXE requer suporte a PnP. O Windows NT 4 não oferece suporte a PnP.

Adição de drivers de adaptadores de rede

Para adicionar drivers de adaptadores de rede

1. Edite o arquivo **ALTDRIVERS.INI** (na pasta ..\ManagementSuite\).
2. Edite o arquivo **NIC.TXT** no diretório ..\ManagementSuite\OSD\Utilities.
3. Use **COPYFILE.EXE** para inserir o arquivo de driver .DOS ou .EXE na imagem de inicialização virtual em **..\ManagementSuite\LANDesk\Vboot\LDVBOOT.IMG**
4. Use o **COPYFILE.EXE** para inserir o **NIC.TXT** na imagem de inicialização virtual.

Como editar o arquivo ALTDRIVERS.INI

O ALTDRIVERS.INI é o arquivo de descrição do driver.

Exemplo de entrada:

```
[Adaptadores Intel PRO/1000]
DRIVER=E1000.DOS
PROTOCOL=E1000
```

- A descrição entre colchetes [ ] pode ser qualquer uma. É o texto que aparece no assistente de Distribuição do SO/Tarefas de migração quando um driver de adaptador de rede é selecionado manualmente.
- DRIVER é o driver do adaptador de rede .DOS ou .EXE.
- PROTOCOL geralmente é igual ao nome do driver ou ao nome do fabricante.

Como editar o arquivo NIC.TXT

O NIC.TXT contém informações para detecção de adaptadores de rede. Será necessário editar o NIC.TXT para adicionar informações do adaptador personalizadas. A seguir, um exemplo da entrada:

```
ven=115D "Xircom"
dev=0003 "Xircom CardBus Ethernet 10/100 Adapter"
drv="CBENDIS.EXE"
prot="XIRCOM"
```

Há quatro chaves e valores possíveis:

- **ven** tem quatro caracteres (por exemplo, 1 deve ser 0001); a descrição pode ser qualquer uma.
- **dev** tem quatro caracteres; a descrição pode ser qualquer uma.
- **drv** é o nome do driver; a extensão padrão é .DOS.
- **prot** é o protocolo, geralmente igual ao nome do driver do fabricante.

Como é possível notar no NIC.TXT, nem todos os drivers apresentam todas as chaves.

Como inserir alterações do driver novamente na imagem de inicialização virtual

Para inserir as alterações novamente na imagem de inicialização virtual, use copyfile (copiar arquivo). A sintaxe é:

```
COPYFILE <arq_img> <arq_origem> <arq_destino
```

Exemplo:

```
COPYFILE c:\Arquivos de programas\LANDesk\ManagementSuite\LANDesk\Vboot\LDVBOOT.IMG
c:\Drivers\MYNIC.DOS\Net\Drivers\MYNIC.DOS
```

NOTA: A variável <destfile> não pode conter a designação da letra da unidade.

É necessário copiar o driver do adaptador de rede .DOS ou .EXE em c:\Net\Drivers e o NIC.TXT atualizado para c:\Net

Adição de drivers de adaptador de rede ao ambiente de inicialização PE Windows

Se precisar de adicionar drivers de rede personalizados ao ambiente PE Windows, siga as etapas abaixo.

Para adicionar drivers de rede ao ambiente de inicialização PE Windows

1. Copie os arquivos .INF e .SYS de driver de rede nesta pasta no servidor núcleo:

   ..\ManagementSuite\LANDesk\Vboot\winpedrv

2. Adicione as informações de driver de rede a este arquivo no servidor núcleo (consulte os exemplos de entradas para ver os detalhes):

   ..\ManagementSuite\altdriverspe.ini

Uso da ferramenta de geração de imagem do LANDesk para DOS

NOTA: Se a sua licença incluir o componente da distribuição do SO e da migração de perfil, os arquivos para a ferramenta de geração de imagem do LANDesk são automaticamente instaladas no seu servidor núcleo. Se desejar executar a ferramenta de geração de imagem do LANDesk de um local diferente, será necessário copiar os quatro seguintes arquivos: IMAGEALL.EXE, IMAGE.EXE, RESTALL.BAT e BACKALL.BAT.

A ferramenta de geração de imagem da LANDesk para DOS (IMAGE.EXE) é um utilitário de backup e restauração baseado em DOS que cria um instantâneo de uma partição ou volume inteiro e o salva em um conjunto de arquivos ou o salva diretamente na maioria das unidades CD-R/RW ATAPI. Se alguma coisa acontecer àquela partição ou volume, você pode restaurar a imagem instantânea.

Limitações

O IMAGE.EXE depende do BIOS para processar funções do disco. Se o BIOS de um computador limitar o acesso à unidade de disco rígido por alguma razão e não houver nenhum gerenciador de unidade disponível para corrigir a limitação, o IMAGE.EXE também estará limitado.

Requisitos de sistema

- Computador pessoal compatível com IBM com microprocessador i80386 ou maior
- 16 MB de RAM
- XMS

Introdução

O IMAGE.EXE é instalado como parte da Distribuição de SO do LANDesk no diretório \Arquivos de programa\LANDesk\ManagementSuite\osd\imaging.

Variáveis de ambiente

Você pode usar diferentes variáveis de ambiente com o IMAGE.EXE:

- **IMSG** exibe uma mensagem na tela. Para criar uma mensagem com IMSG, use o comando set (i.e., set imsg=<incluir mensagem de 80 caracteres ou menos aqui>).
- **IBXT** muda o método usado de gravar um conjunto de CDs de forma que o IMAGE.EXE não solicita o último CD durante uma restauração. Defina a IBXT para o valor de 1. (i.é, set ibxt=1). Esta configuração pode não funcionar com todas as unidades de CD-R/RW.
- **IAR** habilita o IMAGE.EXE a responder automaticamente a avisos e mensagens de erro ao criar uma imagem em um arquivo. Defina IAR para Y ou N (i.é, set iar=Y). Com esse parâmetro, todos os avisos de 'Y'es ou 'N'o (Sim ou Não) que exigem que o usuário pressione Enter são respondidos automaticamente. É possível usar errorlevels do DOS em um arquivo de lote para determinar se a operação teve êxito ou falhou.
- **IOBS=A** testa a velocidade da rede e usa o melhor tamanho de buffer para carregar/descarregar uma imagem.

Opções da linha de comandos

Você pode usar as opções de linha de comandos com o IMAGEW.EXE. Separe as opções com espaços e digite-as na ordem abaixo exibida. Use a opção de linha de comando /? para ver uma lista de opções adicionais não explicadas aqui.

Para criar uma imagem compactada em um arquivo

Formato 1: image /Ch# /U d:\filename.img (sem validação)

Formato 2: image /Ch#V d:\filename.img (validação)

Formato 3: image /Ch#VB d:\filename.img (validação byte por byte)

Explicação: Substitua o h pelo número da unidade de disco de origem de 0 a 7 e o sinal # pelo ID de entrada da partição. Para a maioria dos usuários, o ID da partição é um número de 1 a 4 ou, para volumes, um número formatado do tipo 0xPVV onde P é a partição estendida e VV é o número do volume em hexadecimal de 01 a FF.

Se você não souber o ID da partição ou do volume, execute o IMAGE.EXE sem nenhuma opção de linha de comando e selecione Criar imagem (Create Image). A tela que mostra as partições e volumes conterá o ID em parênteses como número hexadecimal. Esse número deve receber o prefixo 0x na linha de comando.

Para criar uma imagem não compactada em um arquivo

Formato 1: image /Ch# /U d:\filename.img (sem validação)

Formato 2: image /Ch#V /U d:\filename.img (validação)

Formato 3: image /Ch#VB /U d:\filename.img (validação byte por byte)

Explicação: O mesmo acima.

Para criar uma imagem compactada em uma unidade de CD

Formato 1: image /Ch# /CDx (ATAPI)

Formato 2: image /Ch# /CDSx (ASPI)

Explicação: As informações de h e de # são as mesmas acima. O x após /CD é o número de unidade do CD a usar. Omita o x (/CD ou /CDS) para obter uma lista dos dispositivos.

Para criar uma imagem não compactada em uma unidade de CD

Formato 1: image /Ch# /U /CDx (ATAPI)

Formato 2: image /Ch# /U /CDSx (ASPI)

Explicação: O mesmo acima.

Para restaurar uma imagem de um arquivo

Formato 1: image /R d:\filename.img (sem validação)

Formato 2: image /RV d:\filename.img (validação se necessária)

Explicação: Restaura a imagem à mesma unidade de disco e local de onde foi feito o backup.

Para restaurar uma imagem de um CD

Formato 1: image /R /CDx (ATAPI)

Formato 2: image /R /CDSx (ASPI)

Explicação: O x após /CD é o número de unidade do CD a usar. Omita o x (/CD ou /CDS) para obter uma lista dos dispositivos.

Para limitar o tamanho do arquivo na criação

Formatar: d:\nomedoarquivo;s

Explicação: Substitua o s após o ";" por 0 ou 2 GB, 1 para 698 MB ou 2 para 648 MB.

Questões importantes

- Ao criar uma imagem, não use a partição da qual o backup está sendo feito como local do arquivo da imagem. Se fizer isso, a partição será atualizada ao mesmo tempo em que o backup ocorrer. Quando a partição for restaurada, o sistema de arquivos não será consistente.
- Ao restaurar uma imagem, não a restaure sobre a partição que contém o arquivo de origem da imagem. Se fizer isso, a restauração sobregravará as estruturas do sistema de arquivos e o próprio arquivo de imagem.

- Após a restauração, o sistema reinicializará. Isso é necessário porque as partições e o sistema de arquivos em uso pelo SO mudaram. Se a reinicialização não ocorrer, o SO considerará que a partição e o sistema de arquivo continuam sendo os mesmos de antes da restauração. Isso pode causar a corrupção dos dados. Você pode cancelar uma restauração de linha de comando com um /RN, mas esse comando só deve ser usado por usuários avançados que tiverem certeza que é seguro não reinicializar.
- Ao fazer uma restauração com linha de comando, a partição restaurada vai para o mesmo número e local físico do disco rígido de onde o backup foi feito. Se tratar-se de um volume e não houver mais a partição estendida no local, a restauração tentará criar a partição estendida original. Se a restauração não conseguir criar a partição estendida, ela será restaurada como partição primária. Se tratava-se de uma partição primária e agora houver uma partição estendida que inclui o local inteiro, ela será restaurada como um volume. Se houver uma partição ou volume ocupando o mesmo local de início da partição a ser restaurada, aparecerá uma mensagem de advertência antes da sobregravação da partição ou volume.
- Para restaurar através de inicialização por CD, é necessário uma unidade de CD ATAPI. Para unidades SCSI, é necessário criar o próprio arquivo CDBOOT.F35 a fim carregar os drivers corretos ASPI de DOS e lançar o IMAGE.EXE através do AUTOEXEC.BAT, se quiser.

Uso da ferramenta de geração de imagem do LANDesk para o Windows

A ferramenta de geração de imagem da LANDesk para Windows (IMAGEW.EXE) é um utilitário de backup e restauração baseado em Windows 32 que cria um instantâneo de uma partição ou volume inteiro e o salva em um conjunto de arquivos ou o salva diretamente na maioria dos tipos de DVD+RW ou CD-R/RW. Se alguma coisa acontecer àquela partição ou volume, você pode restaurar a imagem instantânea.

O IMAGEW.EXE é compatível com a ferramenta de geração de imagem para DOS da LANDesk (IMAGE.EXE).

Versão atualizada do IMAGEW

O LANDesk Management Suite agora inclui uma versão 2 atualizada do IMAGEW, que inclui suporte para o Windows 7. Esta versão salva arquivos de imagem com uma extensão de arquivo diferente e inclui algumas funcionalidades novas. Se você tiver usado a versão 1 do IMAGEW antes, você pode continuar a usá-lo conforme documentado na seção a seguir.

A Versão 2 do IMAGEW é instalado como parte da Distribuição de SO do LANDesk no diretório ..\ManagementSuite\osd\imagew 2.

Para encontrar informações sobre o uso do IMAGEW 2, visite o site da Comunidade de suporte da LANDesk community.landesk.com.

Uso do IMAGEW version 1

As seguintes informações se aplicam ao IMAGEW versão 1.

Limitações

Se for utilizado com Windows 9x/Me, o IMAGEW.EXE requer que o sistema suporte extensões Int 13h. Se o BIOS de um computador limitar o acesso à unidade de disco rígido por alguma razão e não houver nenhum gerenciador de unidade disponível para corrigir a limitação, o IMAGEW.EXE também estará limitado nos SOs específicos.

Requisitos de sistema

- Computador pessoal compatível com IBM com microprocessador i80386 ou maior
- Ambiente baseado em Windows 32 com o mínimo recomendado de 32 MB de RAM

- Privilégios de Administrador no Windows

O IMAGEW.EXE é instalado como parte da Distribuição de SO do LANDesk no diretório \Arquivos de programa\LANDesk\ManagementSuite\osd\imaging.

Criação de imagens

Há variáveis de ambiente e opções de linha de comando que lhe permitem criar imagens que atendam as suas necessidades.

Variáveis de ambiente

As variáveis de ambiente para o IMAGEW.EXE devem ser usada com opções de linha de comando. As seguintes variáveis de ambiente estão disponíveis:

- **IBXT** muda o método usado de gravar um conjunto de CDs de forma que o IMAGEW.EXE não solicita o último CD durante uma restauração. Defina a IBXT para o valor de 1. (i.é, set ibxt=1). Esta configuração pode não funcionar com todas as unidades de CD-R/RW.
- **IAR** habilita o IMAGEW.EXE a responder automaticamente a avisos e mensagens de erro ao criar uma imagem em um arquivo. Defina IAR para Y ou N (i.é, set iar=Y). Com esse parâmetro, todos os avisos de 'Y'es ou 'N'o (Sim ou Não) que exigem que o usuário pressione Enter são respondidos automaticamente. É possível usar errorlevels do DOS em um arquivo de lote para determinar se a operação teve êxito ou falhou.

Opções da linha de comandos

Você pode usar as opções de linha de comandos com o IMAGEW.EXE. Separe as opções com espaços e digite-as na ordem abaixo exibida. Use a opção de linha de comando /? para ver uma lista de opções adicionais não explicadas aqui.

Para criar uma imagem compactada em um arquivo

Formato 1: imagew /Ch# /U d:\filename.img (sem validação)

Formato 2: imagew /Ch#V d:\filename.img (validação)

Formato 3: imagew /Ch#VB d:\filename.img (validação byte-por-byte)

Explicação: Substitua o h pelo número da unidade de disco de origem de 0 a 7 e o sinal # pelo ID de entrada da partição. Para a maioria dos usuários, o ID da partição é um número de 1 a 4 ou, para volumes, um número formatado do tipo 0xPVV onde P é a partição estendida e VV é o número do volume em hexadecimal de 01 a FF.

Se você não souber o ID da partição ou do volume, execute o IMAGEW.EXE sem nenhuma opção de linha de comando e selecione Criar imagem (Create Image). A tela que exibe as partições e volumes conterá também o ID entre parênteses como um número hexadecimal. Esse número deve receber o prefixo 0x na linha de comando.

Para criar uma imagem não compactada em um arquivo

Formato 1: imagew /Ch# /U d:\filename.img (sem validação)

Formato 2: imagew /Ch#V /U d:\filename.img (validação)

Formato 3: imagew /Ch#VB /U d:\filename.img (validação byte-por-byte)

Explicação: O mesmo acima.

Para criar uma imagem compactada em uma unidade de CD

Formato 1: imagew /Ch# /CDx

Explicação: As informações de h e de # são as mesmas acima. O x após /CD é o número de unidade do CD a usar. Omita o x para obter uma lista dos dispositivos.

Para criar uma imagem não compactada em uma unidade de CD

Formato 1: imagew /Ch# /U /CDx

Explicação: O mesmo acima.

Para restaurar uma imagem de um arquivo

Formato 1: imagew /R d:\filename.img (sem validação)

Formato 2: imagew /RV d:\filename.img (validação se necessária)

Explicação: Restaura a imagem à mesma unidade de disco e local de onde foi feito o backup.

Para restaurar uma imagem de um CD

Formato 1: imagew /R /CDx

Explicação: O x após /CD é o número de unidade do CD a usar. Omita o x para obter uma lista dos dispositivos.

Para limitar o tamanho do arquivo na criação

Formatar: d:\nomedoarquivo;s

Explicação: Substitua o s após o ";" por 0 ou 2 GB, 1 para 698 MB ou 2 para 648 MB.

Questões importantes

- Para executar com o Windows NT/2000/XP Pro, é necessário ter privilégios de administrador. No Windows 2000/XP, pode ser executado como qualquer usuário clicando com o botão direito do mouse e selecionando a opção Executar como (Run As).
- Ao criar uma imagem, não use a partição da qual o backup está sendo feito como local do arquivo da imagem. Se fizer isso, a partição será atualizada ao mesmo tempo em que o backup ocorrer. Quando a partição for restaurada, o sistema de arquivos não será consistente.
- Se você criou um backup sem obter um bloqueio, o backup pode não estar em estado consistente se ocorrerem atualizações à unidade durante o backup.
- Ao restaurar uma imagem, não a restaure sobre a partição que contém o arquivo de origem da imagem. Se fizer isso, a restauração sobregravará as estruturas do sistema de arquivos e o próprio arquivo de imagem.
- Após a restauração, o sistema pode precisar reinicializar. Isso é requerido sob certas condições e determinado pelo programa. Se você não reinicializar quando solicitado, o SO considerará que a partição e o sistema de arquivos continuam da forma como se encontravam antes da restauração, podendo causar a corrupção dos dados. Você pode cancelar uma restauração de linha de comando com um /RN, mas esse comando só deve ser usado por usuários avançados que tiverem certeza que é seguro não reinicializar.

- Ao fazer uma restauração com linha de comando, a partição restaurada vai para o mesmo número e local físico do disco rígido de onde o backup foi feito. Se tratar-se de um volume e não houver mais a partição estendida no local, a restauração tentará criar a partição estendida original. Se a restauração não conseguir criar a partição estendida, ela será restaurada como partição primária. Se tratava-se de uma partição primária e agora houver uma partição estendida que inclui o local inteiro, ela será restaurada como um volume. Se houver uma partição ou volume ocupando o mesmo local de início da partição a ser restaurada, aparecerá uma mensagem de advertência antes da sobregravação da partição ou volume.
- Para restaurar através de inicialização por CD, é necessário uma unidade de CD ATAPI. Para unidades SCSI, é necessário criar o próprio arquivo CDBOOT.F35 a fim carregar os drivers corretos ASPI de DOS e lançar o IMAGEW.EXE através do AUTOEXEC.BAT, se quiser.

Compreensão do ambiente de pré-inicialização do Windows PE

O Windows PE é um sistema mini-Windows que fornece serviços limitados com base nos kernels do Windows. Ele é um ambiente do Windows independente de hardware que contém o seguinte:

- Um subconjunto de APIs do Microsoft Win32.
- Um intérprete de comandos capaz de executar arquivos de lote.
- Suporte para inserção de Windows Script Host (WSH), aplicativos HTML (HTA) e Microsoft ActiveX Data Objects (ADO) para criar ferramentas ou scripts personalizados.

O Windows PE usa o TCP/IP para fornecer acesso à rede e suporta o mesmo conjunto de drivers de dispositivos de rede e armazenamento em massa que o Windows. Algumas limitações não valem nada se a conectividade for limitada somente a conexões de saída (compartilhamento de recursos desativado) e para prevenir o uso do SO pelo cliente, uma reinicialização bem codificada ocorrerá depois de 24 horas de uso.

A LANDesk personalizou o sistema operacional Windows PE somente para incluir as bibliotecas, utilitários e drivers necessários. Além disso, os arquivos do agente LANDesk foram copiados para a imagem para facilitar a funcionalidade LANDesk. Também, o arquivo de comando carregado inicialmente pelo sistema operacional PE foi modificado para incluir os comandos das etapas LANDesk. A partir do Service Pack 2 para o LANDesk 8.7 foi adicionado o suporte WMI à imagem.

Esta seção fornecerá uma lista de arquivos que foram adicionados ou modificados na imagem PE, uma visão geral do processo de inicialização e uma explicação de cada linha no arquivo de comando de inicialização.

Arquivos modificados ou adicionados à imagem do WinPE

Além dos drivers, a imagem do Windows PE do LANDesk inclui os seguintes arquivos modificados ou adicionados.

Arquivo	Objetivo
winbom.ini	Desativa o firewall do Windows PE
\i386\txtsetup.sif	Arquivo de assinatura de LANDesk
\i386\system32\winpeshl.ini	Define a localização do shell
\i386\system32\peshell.exe	O shell usado atualmente

Arquivo	Objetivo
\i386\system32\setupreg.hiv	Inclui o caminho LANDesk
\i386\system32\startnet.cmd	Arquivo de comando executado na inicialização
\i386\system32\all.reg	Modificações de registro de LANDesk
\i386\system32\winpe.bmp	Papel de parede de LANDesk
\CBA8	Agente LANDesk:
\LDCLIENT	Agente LANDesk:

Processo de inicialização do WinPE da LANDesk

O processo de inicialização do WinPE começa assim:

1. Uma vez carregado o setor de inicialização, o SETUPLDR usa o NTDETECT.COM para analisar o hardware para que o HAL correto possa ser carregado.
2. O WINPEOEM.SIF é usado para carregar os drivers de inicialização (os administradores podem personalizar este arquivo para controlar quais drivers de armazenamento em massa serão carregados) e o NTOSKRNL.EXE finaliza a configuração do ambiente e chama o SMSS, que carrega novamente o registro e chama o Winlogon.
3. O Winlogon inicia os serviços, finaliza o carregamento do driver e inicia uma sessão de usuário.
4. O CMD.EXE é executado e processa o STARTNET.CMD. Este arquivo de lote é usado para carregar os drivers da rede e quaisquer outros comandos adicionados a ele. O PE STARTNET.CMD original do Windows se parece com isso:

   ```
   factory winpe
   ```

A imagem do WinPE modificada pela LANDesk por padrão, inclui um arquivo STARTNET.CMD. Na versão 8.7sp2, tem algo assim:

```
@echo off
set path=%path%;x:\cba8;x:\ldclient
\ldclient\GetBootOptions set /a err = %errorlevel%
if %err% gtr 0 goto nofix
ldclient\Diskinfo fix
:nofix
factory winpe
reg import all.reg
\ldclient\wait4ip /t 180
if %errorlevel% gtr 0 goto fail
CD \CBA8
RESIDENTAGENT.EXE /register
RESIDENTAGENT.EXE /start
CD \ldclient
winpepds /install
winpepds /start
if %err% gtr 0 goto nofix
miniscan /nodeviceid /usemacasname
Goto end
:pxe
if %err% lss 2 goto pxemenu
:pxeboot
miniscan /x /nodeviceid /usemacasname
goto end
```

```
:pxemenu
miniscan /nodeviceid /usemacasname
Replcore PxeMenuStart.cmd
call PxeMenuStart.cmd
goto end
:fail
@echo "Failed to get localhost IP address or resolve core server name. Please check your network and try
again."
@pause
:end
```

Definições dos comandos do STARTNET.CMD

A seção seguinte descreve cada linha no STARTNET.CMD.

@echo off

Oculta a saída deste arquivo CMD. REM este comando sai quando um problema é solucionado no STARTNET.CMD.

set path=%path%;x:\cba8;x:\ldclient

Define o caminho para incluir os arquivos adicionados dos agentes LANDesk.

\ldclient\GetBootOptions

Este executável define o nível de erro para 0, 1 ou 2. Os valores são 0, se a máquina for inicializada virtualmente, 1 se a máquina foi inicializada por PXE e o menu PXE foi selecionado e 2, se a máquina foi inicializada por PXE e foi selecionada a inicialização gerenciada.

set /a err = %errorlevel%

Define a variável ERR para o valor derivado de GetBootOptions.

if %err% gtr 0 goto nofix

Esta linha possui o script para pular para a próxima linha se a máquina foi inicializada pelo PXE.

\ldclient\Diskinfo fix

Esta linha somente é processada se não houver inicialização por PXE. O Diskinfo.exe usado com o switch de correção redefine o MBR para inicializar de volta na partição ativa original. O Vbooting foi definido anteriormente nesta inicialização para a unidade RAM WinPE.

factory –winpe

O comando FACTORY.EXE é usado para carregar os drivers e quando chamado com o switch –winpe gerará um nome único para a sessão PE (normalmente minint-<random suffix>) e processar o WINBOM.INI, que é onde você pode configurar e adicionar à ação PE. Por exemplo, já que por padrão, o FACTORY.EXE analisa todos os drivers disponíveis para encontrar um compatível com o hardware descoberto, você pode limitar o número de drivers analisados (e com isso aumentar a velocidade da inicialização) modificando a seção NetCards no arquivo WINBOM.INI.

reg import all.reg

Importa as configurações do ambiente LANDesk para o registro WinPE. Especificamente, o nome do servidor núcleo e a porta usada para o inventário são definidos no arquivo ALL.REG. Eis um exemplo do ALL.REG:

```
Windows registry Editor version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Intel\LANDesk\wuser32]
"CoreServer"="<core_name>"
```

```
"InventoryServerPort"="5007"
```

\ldclient\wait4ip /t 180

O executável wait4ip assegura que tenhamos um endereço IP antes de reunir o inventário para esta máquina. /t 180 define um tempo limite de 3 minutos. Um /s pode ser adicionado para silenciar a saída deste programa. Informações adicionais estão disponíveis executando com um /?.

if %errorlevel% gtr 0 goto fail

Ignora todos os comandos neste arquivo se um endereço IP não pode ser obtido.

CD \CBA8

Altera o diretório de X:\i386\system32 para X:\CBA8.

residentagent.exe /register

O RESIDENTAGENT.EXE é o serviço que escuta em busca de e aceita conexões para comandos remotos, iniciando o aplicativo necessário para lidar com a solicitação (que é como as operações de geração de imagem do LANDesk são executadas). O switch /register instalará e registrará o RESIDENTAGENT.EXE como um serviço. Está conectado no diretório CBA8 no RESIDENTAGENT.LOG.

residentagent.exe /start

O switch /start iniciará o serviço RESIDENTAGENT.EXE, que prosseguirá carregando as bibliotecas necessárias. Este também está conectado no RESIDENTAGENT.LOG.

CD \LDClient

Altera o diretório de X:\CBA8 para X:\LDClient.

winpepds /install

WINPEPDS é o módulo que recebeu ping do servidor núcleo para descobrir esta máquina, verificando se este é o nó gerenciado correto. O switch /install instalará o serviço.

winpepds /start

O switch /start inicia o serviço WINPEPDS.

if %err% gtr 0 goto pxe

Esta linha significa que as máquinas inicializadas com o PXE continuarão o script na seção PXE seguinte.

miniscan /nodeviceid /usemacasname

Esta linha só é executada pelas máquinas inicializadas virtualmente e seu último comando. Miniscan é o utilitário usado para capturar informações mínimas sobre o sistema e o armazenamento no banco de dados do inventário LDMS. A execução do miniscan sem switches incluirá um nome de dispositivo e ID na sua análise de arquivo e será exibido no console como "minint-<random suffix>". Contudo, o uso dos switches /nodeviceid /usemacasname remove esta informação do arquivo de análise e limita os dados enviados em três coisas: Endereço MAC, Endereço IP e Contagem do processador. No console, esses dispositivos aparecem nomeados depois de seus endereços MAC.

if %err% lss 2 goto pxemenu

Diz às máquinas inicializadas por PXE que supostamente devem obter o menu para pular a seção PXEmenu.

miniscan /x /nodeviceid /usemacasname

Esta linha é executada por aquelas máquinas inicializadas por PXE que possuem inicialização gerenciada. Se o /x for usado ao chamar um miniscan, um atributo extra é enviado à porção da rede do arquivo de análise, Pxeboot=Yes.

miniscan /nodeviceid /usemacasname

Esta linha somente é executada pelas máquinas inicializadas por PXE exibidas em um menu. Miniscan é o utilitário usado para capturar informações mínimas sobre o sistema e o armazenamento no banco de dados do inventário LDMS. A execução do miniscan sem switches incluirá um nome de dispositivo e ID na sua análise de arquivo e será exibido no console como “minint-<random suffix>”. Contudo, o uso dos switches /nodeviceid /usemacasname remove esta informação do arquivo de análise e limita os dados enviados em três coisas: Endereço MAC, Endereço IP e Contagem do processador. No console, esses dispositivos aparecem nomeados depois de seus endereços MAC.

replCore PxeMenuStart.cmd

REPLCORE.EXE é usado parra substituir a variável %CoreServer% no arquivo e é apontada para o valor encontrado na chave do registro HKLM\Software\Intel\LANDesk\LDWM\CoreServer (isto foi preenchido com o ALL.REG anteriormente no processo). Neste caso, o PxeMenuStart.cmd está prestes a ser chamado e usa o sdclient para entrar em contato com o servidor núcleo e por isso, deve ter o nome núcleo correto na linha de comando.

call PxeMenuStart.cmd

Se a opção do menu for escolhida pela máquina inicializada por PXE, o PXEMENUSTART.CMD será executado. Duas linhas muito importantes são:

```
sdclient /f /o /p=”http://%CoreServer%/landesk/files/dosmenu.cfg”
RunBatch 500 X:\LDClient PxeMenu dosmenu.cfg
```

Primeiro, o sdclient é usado para recuperar o DOSMENU.CFG no servidor núcleo. Então o RunBatch (um simples utilitário que chama um processo depois de um atraso definido) é usado para carregar o PXEMENU.EXE com os parâmetros do DOSMENU.CFG.

@echo "Failed to get localhost IP address or resolve core server name. Please check your network and try again."

Se um endereço IP não puder ser obtido, esta mensagem de erro aparecerá indicando que o NIC ou os drivers dele devem ser investigados.

Provisionamento

Visão geral do provisionamento

O provisionamento LANDesk permite definir todos os atributos e recursos de novos dispositivos antes de serem apresentados no seu ambiente. O provisionamento usa automação para aplicar esse conjunto de atributos e recursos aos disposição. Com o provisionamento é possível reduzir o tempo ocioso e garantir que os dispositivos sejam confiáveis e previsíveis ao entrarem no ambiente de produção. É possível acessar o histórico de provisionamento de cada dispositivo para descobrir quando e com o que foi provisionado e, se necessário, retornar a um estado anterior. O provisionamento é executado no Windows e no Linuz, não há diferença na criação de modelos entre os sistemas operacionais.

O provisionamento consiste em uma série de ações a serem executadas em um dispositivo alvo. As *ações* são a unidade fundamental do provisionamento. Um *modelo* é uma coleção de ações executadas em uma ordem pré-definida. A LANDesk fornece vários modelos de provisionamento pré-compilados para ajudá-lo a iniciar. Esses modelos são otimizados para trabalhar com configurações específicas de hardware, como sistemas Dell e Hewlett-Packard. É possível combinar esses modelos de provisionamento com seus próprios modelos mestres ou executar modelos com poucas modificações para provisionar genericamente um dispositivo específico das marcas Dell ou HP. É possível dividir as tarefas de provisionamento da mesma forma que se divide o trabalho ao configurar manualmente um sistema.

O provisionamento funciona da mesma maneira, em dispositivos novos ou dinâmicos. Você pode provisionar novos dispositivos com a exata configuração desejada, definindo-a antes da chegada do novo dispositivo. Você pode usar provisionamento para reconfigurar um dispositivo de um propósito para outro, mudando uma função básica do dispositivo para atender às demandas exigentes da sua organização.

Use o alerta para avisar quando ocorre o provisionamento de eventos.

Agente de provisionamento

O centro do provisionamento é o agente ldprovision, localizado na pasta /ldlogon/provisioning. Esse agente consiste em pequenos aplicativos para cada ação. O agente reside no dispositivo alvo. É colocado ali por um servidor PXE ou uma mídia de inicialização física, como uma unidade USB ou um CD.

O processo de provisionamento é terminado quando o agente fizer o seguinte:

- Ele solicita os parâmetros de configuração de um modelo de um serviço Web no servidor núcleo
- Ele verifica o tipo de pré-inicialização para garantir que está sendo executado no ambiente correto de pré-inicialização
- Ele executa as ações na ordem designada na configuração
- Ele reinicializa dispositivo (se necessário)
- Ele injeta uma versão de si mesmo no SO alvo para que poder continuar a funcionar quando o SO real carregar após a reinicialização
- Ele envia feedback para o serviço Web no núcleo

O agente estende as reinicializações necessárias, passando imediatamente para a próxima ação após a reinicialização. A maior parte do trabalho de provisionamento pode ser feito antes de você receber o novo dispositivo. É possível criar um modelo e a tarefa para o modelo executar no novo dispositivo. A tarefa não funcionará até que o agente de provisionamento execute no novo dispositivo.

Para usar um provisionamento completamente, duas permissões são necessários: Provisionamento-agendamento e Provisionamento-configuração. Juntos esses direitos permitem ao usuário criar, editar e agendar modelos de provisionamento. Esses direitos são habilitados automaticamente por quaisquer usuários com direitos Administrativos. Eles podem ser habilitados a quaisquer usuários.

Ferramentas de pré-inicialização

O provisionamento requer a habilidade de inicializar o dispositivo de colocar nele um sistema operacional. Isso pode ser alcançado através do servidor de PXE ou de uma mídia física de inicialização (unidade de CD ou USB). PXE é a maneira mais conveniente de inicializar vários computadores ao mesmo tempo no mesmo ambiente de pré-inicialização. Unidades de CD ou USB são muito portáteis e garantem que o computador executando o ambiente de pré-inicialização é aquele que o administrador deseja provisionar.

O ambiente de pré-inicialização (PE - preboot environment) inclui um sistema operacional completo com vídeo, rede, uma pequena análise de inventário e um agente capaz de receber arquivos e executar comandos. Esse agente executa uma ferramenta de imagem ou ferramenta de instalação de script para instalar o SO no dispositivo. O agente inicia o processo de provisionamento. O provisionamento suporta ambientes de pré-inicialização Windows.

Não é necessário usar mídia única de inicialização para cada sistema do cliente; reuse a mídia de inicialização para outros dispositivos.

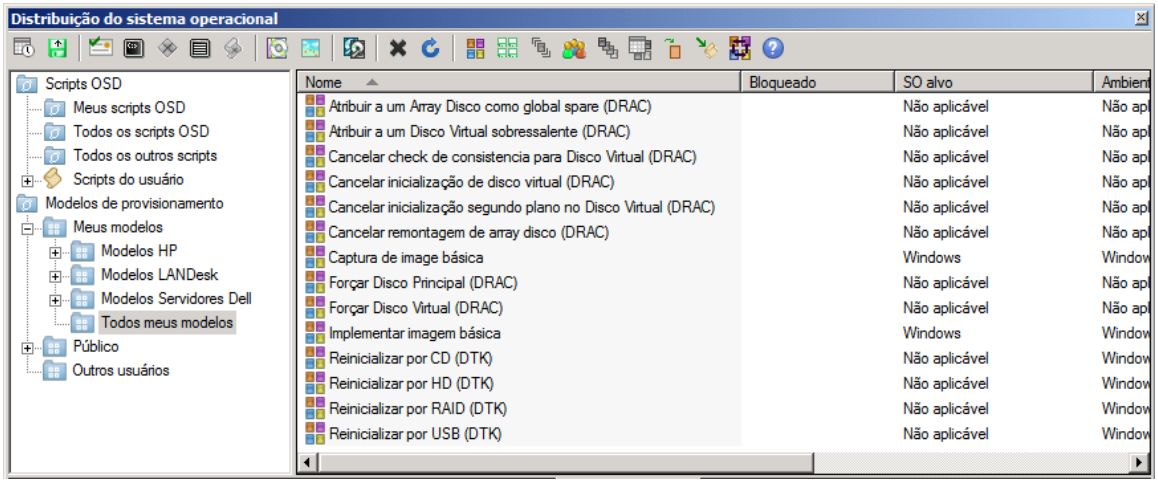
Diferenças entre Distribuição e provisionamento de SO

O provisionamento tem uso mais amplo que a distribuição de SO. A distribuição de SO pode ser parte do processo de provisionamento, mas só é uma parte do provisionamento. O provisionamento inclui o processo do início ao fim de preparação de um dispositivo para uso seguro no seu ambiente. A tabela a seguir mostra como o provisionamento difere da distribuição do SO.

Distribuição do SO	Provisionamento
Originado do núcleo	Originado do dispositivo alvo
Trabalho completado após o dispositivo ter chegado da fábrica	A maioria do trabalho pode ser feita antes da chegada do dispositivo
Só inclui a etapa de distribuição do SO do processo de provisionamento.	Abrange a seqüência de final-a-final da montagem de um dispositivo
Requer uma imagem inteira que não pode ser dividida	Composta de modelos menores, que podem ser modificados ou trocados a nível do modelo

A interface do provisionamento

As ferramentas de provisionamento fazem parte da ferramenta distribuição de sistema operacional (clique em **Ferramentas > Distribuição> Distribuição de SO**). Uma estrutura de árvore exibe modelos de provisionamento e uma barra de ferramentas abre caixas de diálogo para tarefas diferentes.



Na estrutura de árvore, os modelos disponíveis são organizados nas seguintes pastas:

- **Meus modelos:** Os modelos que você criou. Somente você e os usuários administrativos podem ver esses modelos.
- **Público:** Seus modelos e os modelos marcados como públicos.
- **Outros usuários:** (somente usuários administrativos): Uma lista de usuários e seus modelos.

Os modelos públicos são criados pelos usuários com direitos administrativos e podem ser vistos por todos os usuários. O modelos na pasta Meus modelos são visíveis a outros usuários mas só podem ser editados pelo criador ou pelos usuários com direitos administrativos. Toda vez que você usar um modelo não marcado como público, a instância do modelo será bloqueada no histórico. Esta instância não pode ser excluída, mas pode ser ocultada.

O painel direito mostra os modelos da pasta selecionada com cinco colunas que mostram as propriedades do modelo. Clique duas vezes em um modelo para ver sua propriedades completas, inclusive uma lista de outros modelos que incluem o modelo selecionado.

A barra de ferramentas incluem botões para a criação, modificação e gerenciamento de modelos de provisionamento.

- **Novo modelo de provisionamento**: Permite criar um modelo de provisionamento.
- **Criar mídia de inicialização de provisionamento:** possibilita a configuração e criação de mídia de inicialização.
- **Condensar o modelo**: Combina todos os modelos inclusos no modelo selecionado para que haja apenas um arquivo de modelo a executar.
- **Variáveis públicas:** permite ver e configurar variáveis globais aplicáveis a todos os modelos de provisionamento.
- **Criar grupo de modelos**. Permite organizar modelos ao criar grupos dentro de uma pasta.
- **Agendar um modelo:** Abre a ferramenta Tarefas agendadas, que permite ver o provisionamento e outras tarefas de gerenciamento. Você pode agendar tarefas de provisionamento e ver os status das tarefas.
- **Importar modelos:** importa um modelo no banco de dados de núcleo.

- **Instalar scripts:** Disponibiliza os scripts de instalação para uso nas ações de criação de instalação por script e ação de distribuição de imagem nos modelos.
- **Atualizar modelos:** Permite descarregar e importar modelos de LANDesk e configurar o local de download do modelo além das configurações de servidor proxy.

Se você clicar duas vezes em um modelo, a tela Modelo será aberta. Nesta tela, você pode modificar a lista de ações (adicionar ou excluir ações, modificar a ordem das ações e assim por diante). É possível modificar as variáveis que se aplicam especificamente a este modelo e ver e modificar a lista de modelos englobadas por ele ou que o incluem. Você também pode tornar um modelo público, ver seu histórico (quando ele foi executado) e ver ou modificar o código XML do modelo.

Criar e editar modelos de provisionamento

O botão **Novo modelo** é o ponto de início na criação de um novo modelo. Para modificar um modelo, clique com o botão direito no modelo e selecione **Editar**. Para remover um modelo, selecione-o e clique no botão **Excluir**. É possível excluir somente modelos que nunca foram usados.

Criação de grupos de modelos

Você pode usar grupos de provisionamento para organizar modelos de acordo com as suas necessidades. Por exemplo, você pode criar grupos com base em fornecedores específicos e subgrupos adicionais com base nos modelos de dispositivo. É possível criar subgrupos de até seis camadas.

Clonagem de modelos existentes

Uma vez que um modelo é usado, ele não pode ser mudado diretamente. Ele pode ser clonado e depois modificado. Por esta razão, recomendamos que os modelos sejam pequenos. Dessa maneira, se houver necessidade de mudanças, você pode mudar aquele componente da configuração de provisionamento.

A opção **Clonar** faz uma cópia do modelo selecionado. Você pode modificar a cópia, fazer pequenas mudanças na cópia em vez de despender tempo criando um novo modelo inteiro.

Se você fizer a clonagem de um modelo público, a cópia será colocada na pasta Meus modelos e irá adquirir as propriedades de um modelo particular.

1. Clique na pasta **Público** ou **Meus modelos** para mostrar modelos no painel direito.
2. Clique com o botão direito em um modelo e selecione **Clonar**.

   É criada uma cópia do modelo na pasta com o nome padrão do modelo original e a data e hora em que o clone foi criado.

3. Para mudar o nome, a descrição, o ambiente de inicialização ou o SO alvo do modelo clonado, clique com o botão direito no clone, clique em **Propriedades**, modifique as configurações e clique em **OK**.
4. Para modificar as ações, os modelos incluídos, as variáveis de usuário ou o XML do modelo clonado, clique duas vezes no clone para abrir a tela **Modelo**.

Condensar um modelo

Use o botão **Condensar** para combinar vários modelos em um só. Se houver outros modelos inclusos com o modelo atual, o código XML deles será salvo dentro do código XML do modelo para criar um só arquivo XML. Quando você condensa um modelo, ele não pode ser expandido novamente em modelos separados.

Etapas para provisionar um dispositivo

No nível mais básico, o provisionamento de um dispositivo é um processo simples de três etapas. Primeiro, você cria um modelo de provisionamento, em seguida, configura o modelo com os recursos e componentes que desejar instalar no dispositivo e, então, agenda uma tarefa para executar o modelo no dispositivo. Essas etapas são delineadas brevemente aqui; as instruções detalhadas estão disponíveis nas seções seguintes.

Etapa 1: Criar um modelo

Para provisionar um dispositivo, você cria um modelo. Um modelo é um documento XML com uma série de blocos componentes que são aplicados ao dispositivo. Eles são montados uns sobre os outros e podem consistir em ações, atributos, restrições, etc. Um modelo pode ter uma ou várias ações.

Os modelos podem ser encadeados em uma tarefa de provisionamento em uma seqüência em particular. Você pode mudar a ordem da tarefa em um modelo. A sequência pode ser mudada quando aplicável (por exemplo, não é possível colocar uma tarefa pós-SO antes da instalação do SO). Há inúmeros modelos pré-configurados para vários fornecedores (HP, Dell etc.).

Os modelos são salvos como documentos XML no banco de dados.

Etapa 2: Configurar o modelo

Depois que o modelo é criado, ele deve ser configurado com a adição de ações. As ações de modelo são ordenadas em cinco seções. Você só pode selecionar ações em cada seção aplicável à seção (por exemplo, não é possível selecionar Distribuição de software como uma ação para a seção de Pré-instalação). Você pode adicionar qualquer ação disponível a qualquer seção. No entanto, esteja ciente que algumas ações danificarão o modelo ou poderão causar danos ao seu sistema, tornando-o inútil, se completadas em etapas incorretas.

Etapa 3: Agendamento do modelo para distribuição

Uma tarefa de provisionamento contém modelos e os identificadores dos dispositivos alvo. Quando uma tarefa de provisionamento é iniciada, o serviço é associado ao registro de Computador do dispositivo no banco de dados. Isso é necessário para que o histórico de configuração permaneça anexado ao computador. As tarefas de configuração não podem ser reusadas com diferentes dispositivos alvo mas podem ser reusadas especificando-se outro identificador de dispositivo.

A ferramenta **Tarefas agendadas** mostra o status da tarefa agendada enquanto a tarefa está em execução e na sua conclusão. O serviço de agendador possui dois meios de se comunicar com os dispositivos: Através do agente padrão de gerenciamento (que já deve estar instalado nos dispositivos) ou da conta de sistema a nível de domínio. A conta escolhida deve ter o login como privilégio de serviço e você deve ter especificado credenciais no utilitário Configuração de serviços.

Criação de modelos de provisionamento

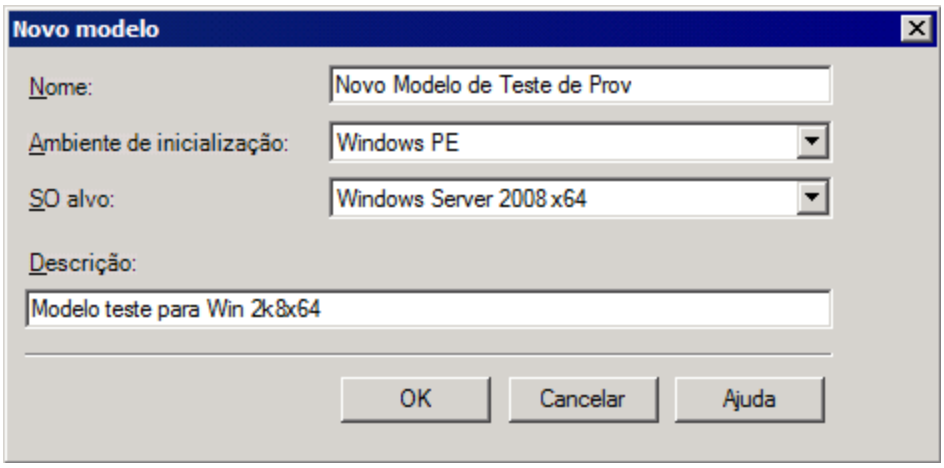
Use o botão da barra de ferramentas **Novo modelo de provisionamento** para criar um modelo de provisionamento

Um modelo é uma série de ações ou blocos componentes a serem aplicados ao servidor em uma ordem em particular. Um modelo pode ter uma ou várias ações. Você pode mudar a ordem da tarefa em um modelo. A seqüência da ação pode ser mudada onde faz sentido, mas não onde não fizer sentido (por exemplo, não é possível colocar uma ação específica que deve acontecer após o SO antes da instalação do SO).

Há inúmeros modelos pré-configurados para vários fornecedores (HP, Dell etc.). Os modelos são armazenados como arquivos XML no banco de dados.

Para criar um modelo

1. Clique em **Ferramentas > Distribuição > Distribuição de SO**.
2. No grupo **Modelos de provisionamento**, selecione a pasta **Público** ou **Meus modelos**.
3. Clique em **Novo provisionamento de modelo** na barra de ferramentas.



4. Digite um nome descritivo na caixa **Nome**.
5. Digite uma descrição na caixa **Descrição**. O Nome e a Descrição são mostrados em colunas na lista de modelos.
6. Selecione o ambiente de inicialização do Windows PE
7. Selecione um sistema operacional alvo para o modelo.
8. Clique em **OK**.

Para mudar as propriedades do modelo, clique duas vezes ou clique com o botão direito no mesmo e selecione **Propriedades**.

Excluir um provisionamento de modelo

Você só pode excluir modelos que não tenham sido executados antes (bloqueado), e somente modelos que não estejam incluídos em outros modelos. Os modelos bloqueados pode ser excluídos (removidos) da tela da lista mas permanecem no banco de dados.

Para excluir um modelo de provisionamento

1. Clique em **Ferramentas > Distribuição > Distribuição de SO**.
2. No grupo **Modelos de provisionamento**, selecione a pasta **Público** ou **Meus modelos**.
3. Selecione um modelo e clique em **Excluir**.
4. Clique em **Sim**.

Configurar um modelo de provisionamento

1. Clique duas vezes em um provisionamento de modelo
2. No painel de navegação esquerdo, clique em **Lista de ações**.
3. No painel central, selecione a seção na qual deseja que a ação ocorra.
    - **Migração do sistema:** Recursos e componentes que precisem ser salvos antes de modificar o sistema (ou migrar um dispositivo para outro hardware ou máquina virtual). Por exemplo, esta seção pode incluir uma ação para capturar informações de perfil quando migrar para o Windows Vista.
    - **Pré-instalação do SO:** Ações que são realizadas quando o dispositivo inicializa no ambiente de pré-instalação (Windows PE). Por exemplo, em um servidor você adicionaria a configuração de RAID nesta seção.
    - **Instalação do SO:** Ações realizadas no ambiente de pré-instalação (Windows PE) quando o SO está instalado.
    - **Pós instalação do SO:** Ações que são realizadas no sistema operacional alvo após ele ter sido instalado, como a execução de uma tarefa de gerenciamento de patch.
    - **Configuração do sistema:** Instalação/execução adicional de aplicativo e configuração do sistema no SO instalado. Por exemplo, adicionar tarefas de instalação de driver nesta seção.
4. Clique em **Adicionar**.
5. Digite um nome específico para a ação no campo **Nome**.
6. Digite uma descrição detalhada da ação no campo **Descrição**.
7. Na lista **Tipo**, selecione um tipo de ação.
8. Em **Variáveis de ação**, clique em **Adicionar** para acrescentar uma variável que se aplica somente a esta ação. Especifique os valores nas caixas de texto, selecione o tipo de variável e clique em **OK**.
9. Em **Propriedades da ação selecionada**, preencha os dados necessários para o tipo de ação. Esses dados variam dependendo do tipo de ação que você selecionar.
10. Quando a ação é definida, clique em **Aplicar** para salavá-la e continue a editar o modelo. Quando você terminar de definir o modelo, clique **OK**.

Agendar uma Tarefa de provisionamento

Para agendar uma tarefa de provisionamento

1. Na ferramenta **Distribuição de sistema operacional**, selecione um modelo de uma das pastas de **Modelos de provisionamento**.
2. Clique no botão **Agendar modelo** na barra de ferramentas.

   A ferramenta Tarefas agendadas abre com uma tarefa para o modelo de provisionamento.
3. Na tela de rede, selecione os dispositivos para os quais você vai distribuir a tarefa de provisionamento. Arraste os dispositivos para a ferramenta **Tarefas agendadas** e solte-as na tarefa de provisionamento.
4. Clique com o botão direito na tarefa de provisinamento e selecione **Propriedades**. Selecione uma opção de agendamento e clique em **Salvar**.

Ao clicar em **Agendar modelo**, é criada uma tarefa (ela não tem dispositivos alvo e é não-agendada). Se você não adicionar dispositivos alvo ou agendar a tarefa, esteja alerta para o fato de que a tarefa permanecerá na lista de tarefas até você agendá-la ou apagá-la.

Na ferramenta **Tarefas agendadas**, as tarefas são agrupadas nas seguintes pastas:

- **Minhas tarefas:** As tarefas que você agendou. Somente você e os usuários administrativos Management Suite podem ver essas tarefas.
- **Tarefas públicas:** Tarefas que os usuários marcaram como públicas. Qualquer pessoa que agendar uma tarefa desta categoria, se tornará o proprietário daquela tarefa. A tarefa permanece na pasta **Tarefas públicas** e também será visível no grupo **Tarefas do usuário** daquele usuário.
- **Todas as tarefas:** Suas tarefas e as tarefas marcadas como públicas.
- **Tarefas do usuário** (Somente para usuários administrativos Management Suite): Todas as tarefas que os usuários tenham criado.

Notificações de usuário durante a execução de uma tarefa

Quando uma tarefa de provisionamento está em execução em um dispositivo e as ações de provisionamento incluem uma reinicialização, a tarefa continua em execução após o reinício. É solicitado que o usuário faça o logon depois da reinicialização, e após a conclusão, uma mensagem de status informa o progresso da tarefa.

Se o usuário não fizer o logon quando a tarefa de provisionamento iniciar, a tarefa executa sem entrada de usuário. Se há uma ação de reinicialização, a tarefa continuará a executar sem o logon do usuário.

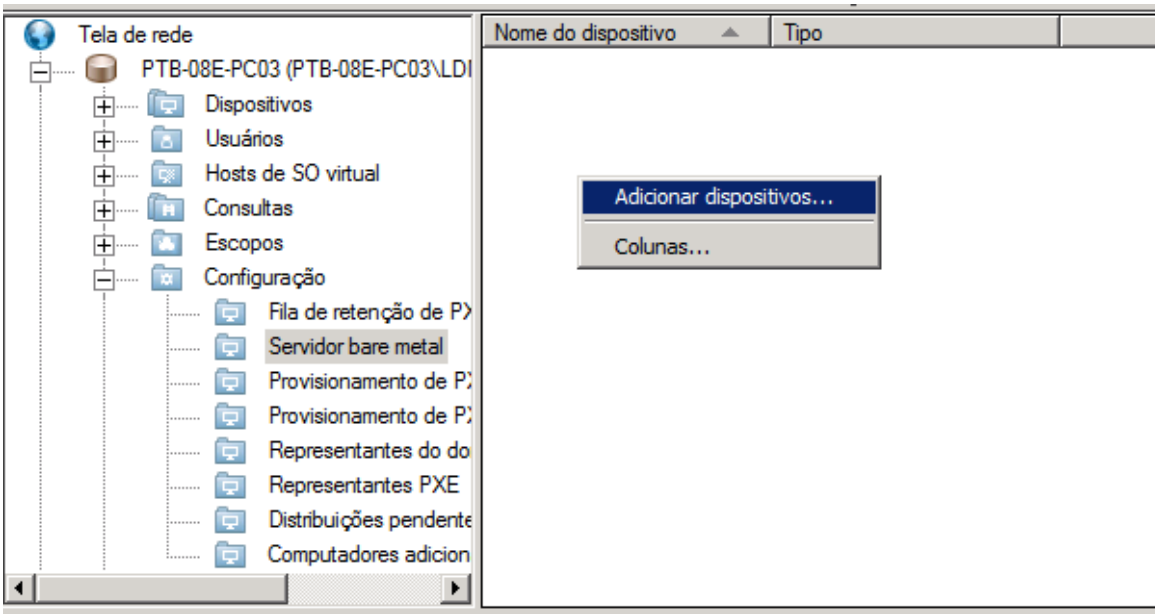
Se o usuário faz logon no dispositivo enquanto a tarefa de provisionamento está em processo, uma mensagem de status informa que uma tarefa está em processo e fornece o progresso da tarefa. As mensagens de status são atualizadas somente entre ações. Se uma tarefa estiver trabalhando em uma ação longa, tal como instalar um aplicativo grande, a barra de progresso pode parece estática. No entanto, quando a ação estiver concluída, o status será atualizado.

Provisionamento de dispositivos bare-metal (Sem SO)

O provisionamento permite o provisionamento de dispositivos bare-metal. Você pode iniciar esse processo antes que o dispositivo esteja fisicamente presente. Para fazer isso, você digita um identificador de hardware (como GUID ou o endereço MAC) para cada novo dispositivo na pasta **Configuração > Servidor Bare-metal** na tela da rede. Você pode adicionar vários dispositivos de uma vez importando uma lista de IDs de dispositivos, usando um arquivo CSV. As informações requeridas pelo agente de provisionamento automatizado (ldprovision) são registradas no banco de dados.

Para provisionar dispositivos bare-metal

1. Na tela de rede, clique em **Configuração > Servidores bare-metal**.
2. Clique com o botão direito no dispositivo e selecione **Adicionar dispositivos**.



3. Para digitar dados para dispositivos individuais, clique em **Adicionar**. Digite um nome para os dispositivos que você adicionará (você pode digitar um nome que descreve um grupo de dispositivos ou apenas um dispositivo).
4. Selecione um tipo na lista **Tipo de identificador**.
5. Digite o identificador para cada dispositivo e clique em **Adicionar** para adicioná-lo à lista.
6. Para importar os dados do dispositivo, selecione um tipo na lista **Tipo de identificador**. Digite a unidade, o caminho e o nome do arquivo a importar e navegue para selecioná-lo. Clique em **Importar**.
7. Associe cada dispositivo com um provisionamento de modelo.
8. Conecte os dispositivos e coloque um CD de inicialização IdProvision, unidade USB inicializável ou configure o BIOS para inicialização em rede/PXE.
9. Ligue os dispositivos.

Criação de mídia de inicialização

Use a caixa de diálogo LANDesk Boot Media Creator (Criador de mídia de inicialização LANDesk) para criar mídia de inicialização que pode ser usada para provisionar dispositivos. O provisionamento cria uma mídia física pela qual iniciar o dispositivo em um ambiente de pré-inicialização. Essa mídia pode ser entregue através de um servidor PXE ou dispositivo inicializável USB/CD/DVD.

Um ambiente de pré-inicialização consiste em um sistema operacional completo com vídeo, rede, uma análise de mini-inventário e um agente capaz de receber arquivos e executar comandos. Para a mídia de inicialização funcionar você precisa configurar o dispositivo alvo para inicializar da mídia adequada (no BIOS, ative a inicialização IPXE por rede ou por CD/DVD).

Para cirar uma imagem de mídia de inicialização

1. Clique em **Ferramentas > Distribuição > Distribuição de SO**.
2. Na barra de ferramentas, clique no botão **Criar mídia de inicialização de provisionamento**.

3. Selecione **Tipo de mídia de inicialização** (ISO ou USB drive reiniciável). Se você selecionar um drive USB, insira-o e selecione a letra do driver. Se você selecionou ISO inicializável, selecione o caminho de destino onde a ISO será salva.
4. Clique em **Criar**.

A criação da mídia inicializável poderá falhar se o sistema possuir pouca memória.

NOTA: Ao criar uma mídia de inicialização USB, você precisa ter direitos de administrador. No caso do Microsoft Vista, você precisa descarregar o programa e executá-lo como administrador.

NOTA: Para criar mídias de ISO, o dispositivo onde você executou a criação de mídia de inicialização precisa ter IMAP2, que é disponível da Microsoft no site http://support.microsoft.com/kb/kb932716.

Compartilhamento de modelos

Use o botão da barra de ferramentas **Importar modelos** para importar modelos no formato .XML. Ao importar um modelo, uma cópia do modelo é gravada na pasta **Meus modelos**. Em seguida, você pode editar XML do modelo para fazer mudanças nele.

Você também pode exportar um modelo para salvá-lo como novo arquivo e compartilhá-lo com outros.

Para importar um modelo

1. Clique em **Ferramentas > Distribuição > Distribuição de SO**.
2. Na barra de ferramentas, clique no botão **Importar modelos**.
3. Digite o caminho e o nome do arquivo arquivo XML na caixa de texto **Importar arquivo** ou clique em **Procurar** e selecione o arquivo.
4. Clique em **Importar**. O modelo será importado na pasta **Meus modelos**.

O arquivo é gravado como arquivo .xtp (página do modelo XML). Na pasta **Meus modelos**, o modelo importado é exibido com o nome de arquivo seguido pela data e hora da importação.

Para exportar um modelo

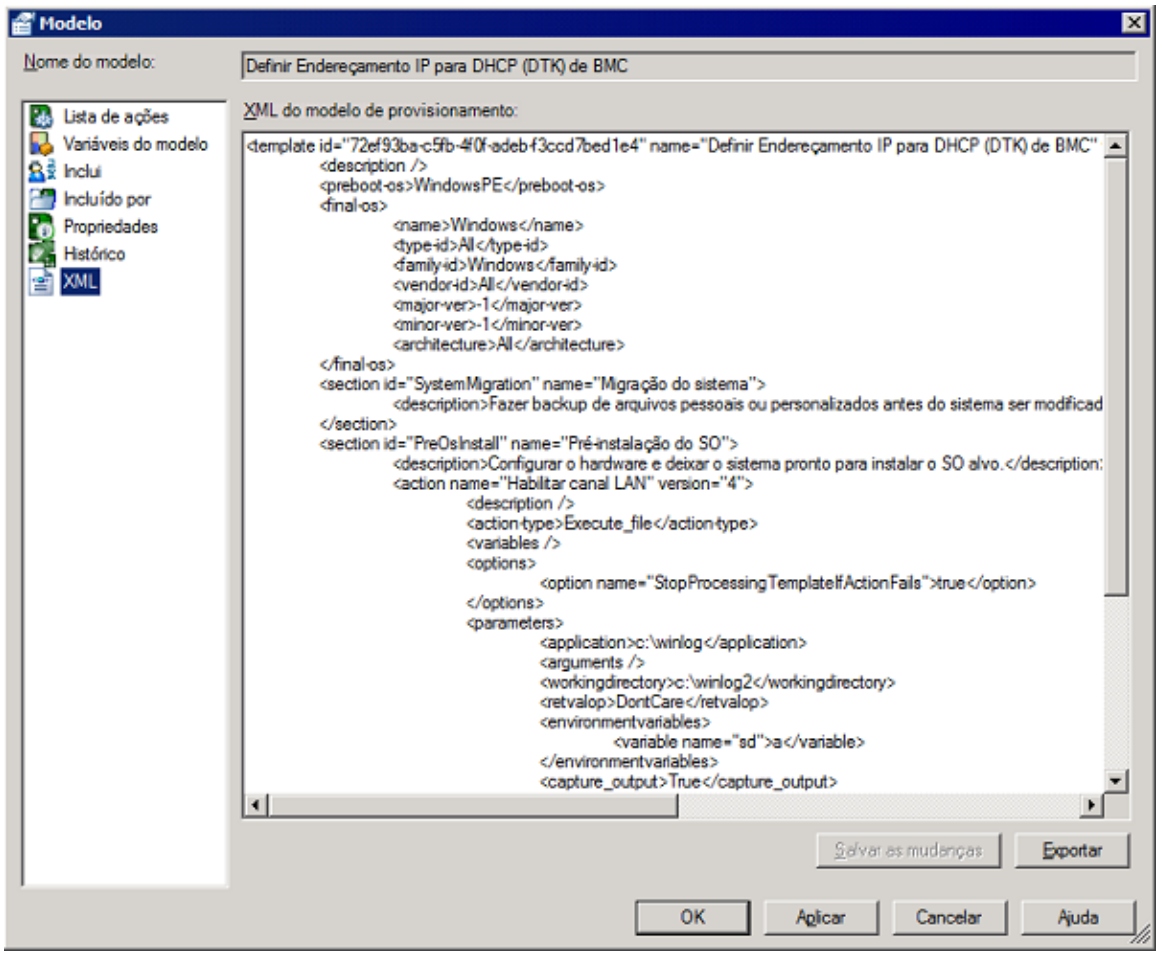
1. Clique em **Ferramentas > Distribuição > Distribuição de SO**.
2. Selecione **Público** ou **Meus modelos** ou um de seus subgrupos.
3. Clique duas vezes em um modelo. Na tela Modelo, clique em **XML**.
4. Clique em **Exportar**. Selecione o local no qual deseja salvar o modelo e clique em **Salvar**.

O arquivo é gravado como arquivo .xtp (página do modelo XML). Se você exportar um modelo que contenha somente caracteres UTF. (O título não será exibido corretamente no Internet Explorer). Os caracteres que não puderem ser exibidos no título do modelo serão mostrados como sublinhados. Você pode mudar o título do modelo utilizando a caixa de diálogo **Salvar como**.

Editar um código XML de um modelo

1. Clique em **Ferramentas > Distribuição > Distribuição de SO**.
2. Selecione **Público** ou **Meus modelos** ou um de seus subgrupos.
3. Clique duas vezes em um modelo. Na tela Modelo, clique em **XML**.

4. Faça as mudanças no código XML do modelo.
5. Para salvar as alterações, clique em **Salvar as alterações**.
6. Para exportar uma cópia do modelo, clique em **Export**ar e especifique um local para o arquivo.
7. Clique em **OK** para fechar a tela Modelo.



Os modelos de provisionamento são estruturados usando o seguinte formato geral XML.

```
<template name= >

    <description></description>

    <section name= >

        <description></description>
        <action></action>

    </section>

    <section name= >

        <description></description>
        <action></action>

    </section>
```

```
</template>
```

Usar modelos pré-definidos

Use o botão **Atualizar modelos** para fazer o download de modelos otimizados pré-definidos para hardwares de sistema específicos e tarefas comuns de provisionamento. Após concluir o download dos arquivos, você pode salvá-los na pasta Meus modelos.

Novos modelos podem tornar-se disponíveis e você pode fazer o download de modelos mais de uma vez se quiser atualizar ou adicionar novos modelos.

Os downloads podem ser feitos a partir dos servidores LANDesk; selecione o servidor mais próximo do seu local. A caixa de diálogo **Atualizar modelos** também permite que você especifique configurações de servidor proxy se você usa um servidor proxy para acesso externo.

NOTA: Quando uma tarefa agendada de atualização de modelo é executada, ela usa as configurações dessa caixa de diálogo que estão atualizadas no momento da atualização, e não as configurações da tarefa quando esta foi criada.

Clique aqui para opções para **Atualizar modelos**

Download da guia de modelos mais recente

- **Selecionar o site da fonte do download:** Especifica qual servidor de conteúdo modelo de provisionamento você acessará para atualizar o seu banco de dados com os modelos de provisionamento mais recentes. Selecione o servidor mais próximo do local onde você se encontra.
- **Selecionar os modelos de provisionamento para atualizar**: Identifica quais modelos de provisionamento de plataforma são atualizados. Você pode selecionar uma ou mais plataformas. Quanto mais plataformas você selecionar, maior será o tempo necessário para o download.
- **Importar como um nova cópia (Criar novos modelos):** Importa os modelos como novos e não sobrescreve modelos ou grupos já existentes.

Guia de configuração do servidor proxy

Se sua rede usa um servidor proxy para transmissões externas (como acesso à Internet), use essa guia para habilitar e definir as configurações do servidor proxy. É necessário acesso à Internet para atualização das informações do modelo de provisionamento.

- **Usar servidor proxy:** Habilita a opção de servidor proxy (por padrão, essa opção é desativada). Se você habilitar um servidor proxy, deverá preencher os campos de endereço e porta abaixo.
  - **Endereço:** Identifica o endereço IP do servidor proxy.
  - **Porta:** Identifica o número de porta do servidor proxy.
- **Proxy baseado em HTTP:** Habilita o servidor proxy, se for baseado em HTTP (como o Squid) para que a conexão e o download dos patches de sites FTP sejam bem-sucedidos. (Os patches baseados em alguns sites FTP não podem ser carregados através de um proxy baseado em HTTP a não ser que esta opção seja habilitada primeiro).
- **Requer login:** Permite digitar um nome de usuário e uma senha se o servidor proxy usa credenciais em vez de ser um servidor proxy transparente.
  - **Nome de usuário:** Digite um nome de usuário válido com credenciais de autenticação para o servidor proxy.
  - **Senha:** Digite a senha do usuário.

Fazer o download e importar modelos pré-definidos

1. Clique em **Ferramentas > Distribuição > Distribuição de SO**.
2. Na barra de ferramentas, clique no botão **Atualizar modelos**.
3. Se necessário, clique na guia **Configurações de servidor proxy** e especifique as configurações de servidor proxy.
4. Selecione um site de fonte de download:
5. Selecione os modelos específicos ao fornecedor que deseja descarregar.
6. Selecione **Importar como nova cópia (cria novos modelos)** para salvar os modelos que foram baixados separadamente, sem sobrescrever nenhum modelo ou grupo existente com o mesmo nome.
7. Clique em **Download**. Uma mensagem é exibida informando que o download dos modelos foi bem sucedido.
8. Clique em **Importar** para mudar os modelos para a pasta **Meus modelos**.

Usar scripts de instalação em provisionamento de modelos

Use **Instalar scripts** para criar um modelo de um ou mais scripts. Essa opção disponibiliza os scripts de instalação para uso nas ações de criação de instalação por script nos modelos. O provisionamento suporta scripts de arquivos de lote, scripts shell e vários outros.

As ações de distribuir imagem, instalar com script e injetar script use os scripts como sysprep.inf ou unattend.txt. A instalação de scripts também pode inserir variáveis nos seus scripts; por exemplo, um nome de dispositivo pode ser inserido em um arquivo sysprep.inf.

Usar variáveis

Os scripts de instalação suportam vários pares de chave importantes, como, por exemplo:

Variável	Descrição
%IdHostname%	O nome do host
%IdDeviceID%	O GUID do dispositivo

Se houver um par de chave importante no arquivo WIN.INF que já existe como variável definida pelo usuário, os Scripts de instalação os substituem com essa variável.

Para passar variáveis por um script de instalação como variáveis (sem serem substituídas pelo processo de provisionamento), delimite-as com sinais duplos de porcentagem, como `%%variável%%`.

Notas sobre uso de scripts

- No Windows, deve haver uma partição válida, ativa e formatada antes da ação de Instalação por script.
- A origem de instalação da rede deve ter drivers para o dispositivo alvo injetado corretamente ou colocado no caminho do driver PnP do OEM (para informações adicionais, consulte a documentação sobre instalação da Microsoft).
- No momento, só funciona a instalação de linha de comando usando o winnt32.
- O arquivo cmdlines.txt é usado para anexar comandos à inicialização final do SO.

- Não há suporte ao PXE/RIS no momento.
- Se a instalação falhar, você pode resolver problemas de erro verificando a pasta \ManagementSuite\ldlogon\provisioning\config para ver o script de instalação com as variáveis substituídas. Esta estratégia se aplica também sempre que você modificar um script ou usar um script nas ações Injetar script e Distribuir imagem.
- O diretório temporário usado para o provisionamento é %systemdrive%/ldprovisioning.

Problemas de instalação do Linux

A instalação por script do Linux é aceita somente através da inicialização de PXE.

Ao executar uma ação de instalação por script no Linux, lembre-se de que cada versão do Linux verifica se você está usando o CD correto no início da instalação. Assim sendo, você precisará de um initrd e linux (vmlinuz) diferente para cada versão do Linux.

A melhor maneira de fazer isso é copiar as imagens de inicialização de cada CD ao PXE e renomeá-las. Você deve copiá-las no caminho \LANDesk\PXE\System\images\x86pc\undi\provlinux. Por exemplo, para o Red Hat 4, renomeie o arquivo como initrd.rh4as e vmlinuz.rh4as e para o Sles10, renomeie os arquivos como initrd.sles10 e linux.sles10. Em seguida, quando criar uma ação de instalação por script, use o initrd.xxx e xxxlinux.xxx corretos no modelo de Instalação por script.

Os scripts de instalação do Linux oferecem suporte a vários pares de chave importantes, como, por exemplo:

Variável	Descrição
ldDNSDomain	O domínio DNS
ldInstallServer	O servidor de origem da instalação
ldInstallDir	O diretório de instalação. Por exemplo, /storage/OS/linux/redhat/enterprise_4as/u3/i386/
ldNameserver1	Servidor de DNS 1
ldNameserver2	Servidor de DNS 2

Importar e exportar scripts de instalação

Para importar um script de instalação

1. Clique em **Ferramentas > Distribuição > Distribuição de SO**.
2. Na barra de ferramentas, clique no botão **Scripts de instalação**.
3. Digite o nome do caminho e do arquivo do script na caixa de texto **Nome do arquivo** ou clique em **Procurar**, navegue até o script, selecione-o e clique em **OK**.
4. Digite um nome para o script na caixa de texto **Nome do script** . Este nome aparece na lista de **Scripts de instalação** nesta caixa de diálogo.

   O nome também é exibido na lista **Scripts de instalação** quando você adiciona um ação de Instalação por script para um modelo de provisionamento.
5. Digite detalhes adicionais sobre o script na caixa de texto **Descrição**.

6. Selecione o sistema operacional alvo na lista suspensa **Sistema operacional alvo**.
7. Selecione a caixa de seleção **Inserir variáveis no script** se quiser trocar variáveis durante a importação do script. Ao substituir as variáveis, as variáveis públicas serão substituídas automaticamente. Há suporte a variáveis personalizadas adicionais. Os valores serão substituídos quando o modelo for executado.
8. Clique em **Importar** para colocar o script na lista **Scripts de instalação**.

Para exportar um script de instalação

1. Na caixa de diálogo **Scripts de instalação**, selecione o script na lista **Scripts de instalação**.
2. Clique em **Exportar**. Especifique um nome de arquivo e local e clique em **Salvar**.

Histórico do provisionamento

A opção histórico de provisionamento permite que você veja a história de um modelo de provisionamento. Você pode verificar o status de uma tarefa em particular, determinar como um servidor específico foi provisionado ou descobrir quais servidores foram provisionados com um modelo em particular. Quando um sistema é provisionado, todas as ações são registradas no histórico de provisionamento.

Se desejar colocar um sistema de volta em um estado conhecido, você poderá executar novamente o modelo que permite voltar a tal estado. Para executar novamente um modelo, lembre-se de que algumas ações são externas ao provisionamento. Salve todos os pacotes de distribuição de software, as configurações de agente e os programas que baixou e executou em conjunto com um modelo. Se não o fizer, não será possível executá-los novamente.

Para ver o histórico de provisionamento de um modelo

1. Clique em **Ferramentas > Distribuição > Distribuição de SO**.
2. Em **Modelos de provisionamento**, clique nas pastas **Público** ou **Meus modelos** para mostrar os modelos.
3. Clique duas vezes em um modelo.
4. Clique em **Histórico**.
5. Clique em um nome na coluna **Nome da tarefa** e clique em **Selecionar** para ver detalhes sobre aquela tarefa.

NOTA: Se o modelo nunca foi executado, não há histórico.

Para ver o histórico de provisionamento por tarefa

1. Clique em **Ferramentas > Distribuição > Tarefas agendadas**.
2. Em **Minhas tarefas** ou **Tarefas públicas**, clique no nome da tarefa.
3. Clique em uma categoria sob a tarefa (Todos os disposivos, Ativo, Pendente, Bem sucedido ou Falhou). Os dispositivos alvo estão relacionados nessas categorias dependendo do status da tarefa de provisionamento no dispositivo.
4. Clique com o botão direito em um dispositivo alvo e selecione **Histórico de provisionamento**.
5. Clique em **Propriedades** para ver as propriedades do modelo de provisionamento.
6. Expanda uma seção de modelo e clique em uma ação para ver os detalhes da distribuição da ação.

Para ver o histórico de provisionamento por dispositivo

1. Na tela de rede, clique em **Meus dispositivos** ou **Dispositivos públicos** e encontre o dispositivo.
2. Clique com o botão direito no dispositivo e selecione **Histórico de provisionamento**.
3. Clique um nome de tarefa e clique em **Selecione** para ver os detalhes da tarefa de provisionamento.
4. Clique em **Propriedades** para ver as propriedades do modelo de provisionamento.
5. Expanda uma seção de modelo e clique em uma ação para ver os detalhes da distribuição da ação.

NOTA: Para obter o status atual de um modelo que está em processo de execução, clique no botão **Atualizar** para atualizar o status do histórico.

Grupos de Modelos de provisionamento

Use grupos de modelos de provisionamento para organizar seus modelos de diversas formas. Por exemplo, você pode criar grupos com base em fornecedores específicos e subgrupos adicionais com base nos modelos de dispositivo. Mais tarde, se quiser modificar um dos modelos no grupo, você só precisa remover o modelo do grupo e adicioná-lo novamente ao grupo depois de modificado. É possível criar subgrupos de até seis camadas.

Para criar um grupo de modelos

1. Clique em **Ferramentas > Distribuição > Distribuição de SO**.
2. Selecione a pasta **Público** ou **Meus modelos**.
3. Clique no botão **Criar grupo de modelos** na barra de ferramentas.
4. Digite o nome do grupo na caixa **Nome do grupo**.
5. Digite uma descrição no campo **Descrição de grupo**.
6. Clique em **OK**.

Para excluir um grupo

1. Selecione um grupo e clique no botão **Excluir** na barra de ferramentas.
2. Clique em **Sim** e, em seguida, confirme a exclusão do grupo.

NOTA: Um grupo pode ser excluído mesmo se não estiver vazio. Verifique se todos os subgrupos ou modelos no grupo podem ser excluídos antes de confirma a exclusão.

Definir o locar para armazenamento da imagem e ferramenta

Use a caixa de diálogo **Escolher local de armazenagem de armazenamento e ferramenta de imagem** para indicar onde está localizada a ferramenta de imagem e onde deseja armazenar a imagem. Essa caixa de diálogo está disponível como parte das ações **Capturar imagem** e **Distribuir imagem**.

Para definir o local da imagem e da ferramenta

1. Clique em **Ferramentas > Distribuição > Distribuição de SO**.
2. Em **Provisionamento de modelos**, clique em **Público** ou **Meus modelos**.
3. Clique duas vezes em um modelo.
4. Clique em **Lista de ação**.

5. Clique na seção **Instalação do SO**.
6. Clique no botão **Adicionar**.
8. Na lista **Tipo de ação**, selecione **Capturar imagem** ou **Distribuir imagem**. Digite um nome para a ação e clique em **OK**.
9. Clique em **Iniciar assistente**.
10. Na lista **Selecionar tipo de imagem**, selecione o tipo de imagem que desejar capturar ou distribuir.
11. Especifique o local onde deseja salvar o arquivo de imagem.
12. Especifique o local do aplicativo de imagem.
13. Clique em **OK**.

NOTA: Frequentemente, as imagens são salvas em um local diferente do servidor núcleo. Se esse for o caso, as ações **Capturar imagem** ou **Distribuir imagem** devem ser precedidas pela ação **Mapear unidade**, na qual você especifica as credenciais de autenticação do local.

Provisionamento de variáveis de modelo

As variáveis de modelo fornecem maior portabilidade e personalização nos modelos. Por exemplo, um modelo pode conter nomes de arquivos específicos para cópia, caminhos de instalação ou um endereço IP do qual exportar arquivos. Com as variáveis de usuário nesses itens específicos, o modelo pode abordar mais situações ou locais porque você pode simplesmente trocar as variáveis no código XML e substituir os itens especificados.

Existem quatro tipos de diretiva: Elas são (em ordem de precedência)

- **Dispositivo:** Variáveis atribuídas a um dispositivo específico
- **Global:** Variáveis que são públicas (disponível) para todos os modelos
- **Modelos:** Variáveis que se aplicam somente ao modelo atribuído
- **Ação:** Variáveis que se aplicam somente a uma ação

Variáveis que são sensíveis a maiúsculas/minúsculas.

Tópicos relacionados

"Definir uma variável de dispositivo " na página 440

"Definir uma variável públicas (global)" na página 440

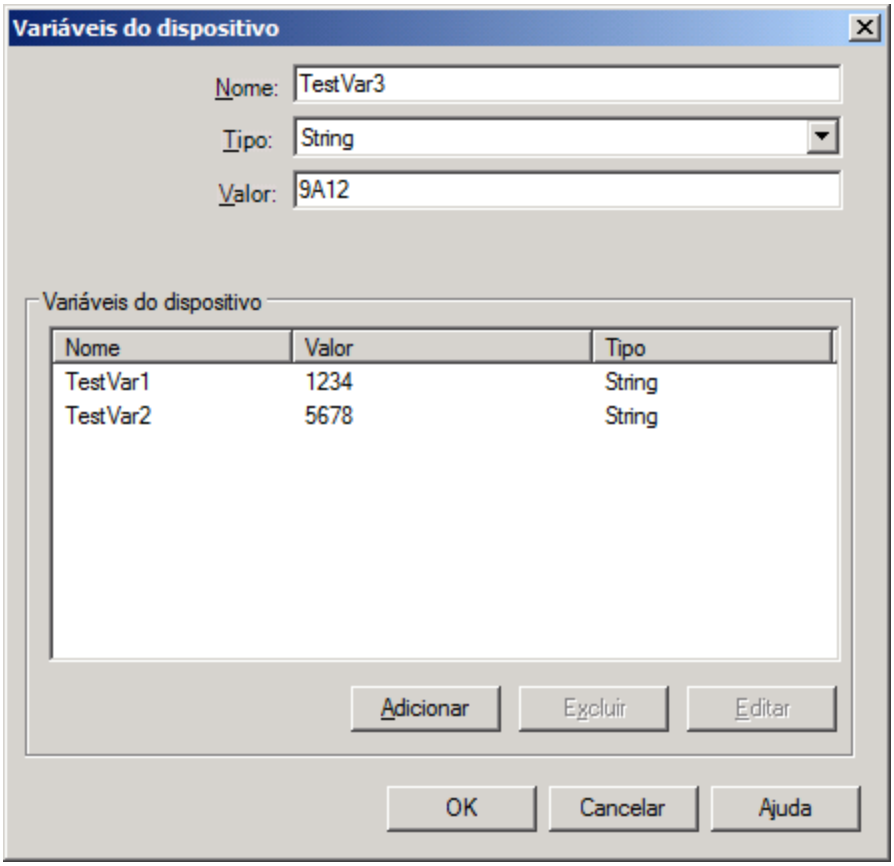
"Definir uma variável de modelo" na página 442

"Definir uma variável de ação" na página 443

"Criar identificadores exclusivos para novos dispositivos " na página 444

Definir uma variável de dispositivo

1. Na lista **Todos os dispositivos**, clique com o botão direito e selecione **Gerenciar variáveis**.



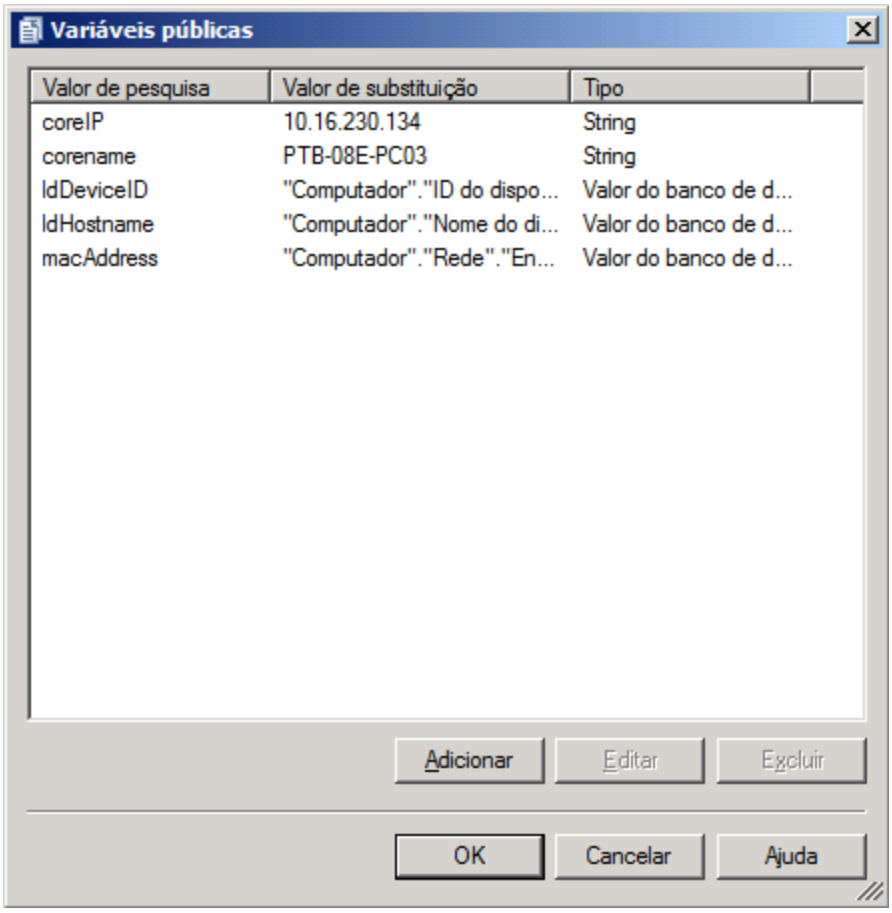
2. Digite o nome do item (como endereço IP) no campo **Nome**.
3. Digite o valor a ser substituído na caixa de texto **Valor**.
4. Selecione o tipo.
   - **String:** Digite um valor de string
   - **Valor de banco de dados:** Digite uma string de ID de banco de dados como Computer.Network."NIC Address"
   - **Dados sensíveis:** Digite o valor a ser criptografado no banco de dados.

   Use aspas para os nomes com espaços. A maioria dos valores do banco de dados de inventário pode ser usada.
5. Clique em **Salvar**.

Definir uma variável públicas (global)

Use o botão da barra de ferramentas **Variáveis públicas** para ver e configurar variáveis globais e aplicá-las a todos os modelos de provisionamento. Essas variáveis são usadas para personalizar nomes de arquivos de modelos, caminhos de instalação ou endereços IP dos quais arquivos serão exportados. As variáveis de usuário (variáveis que só se aplicam a um modelo) prevalecem sobre as variáveis públicas.

1. Clique em **Ferramentas > Distribuição > Distribuição de SO**.
2. Na barra de ferramentas, clique no botão **Variáveis públicas**.



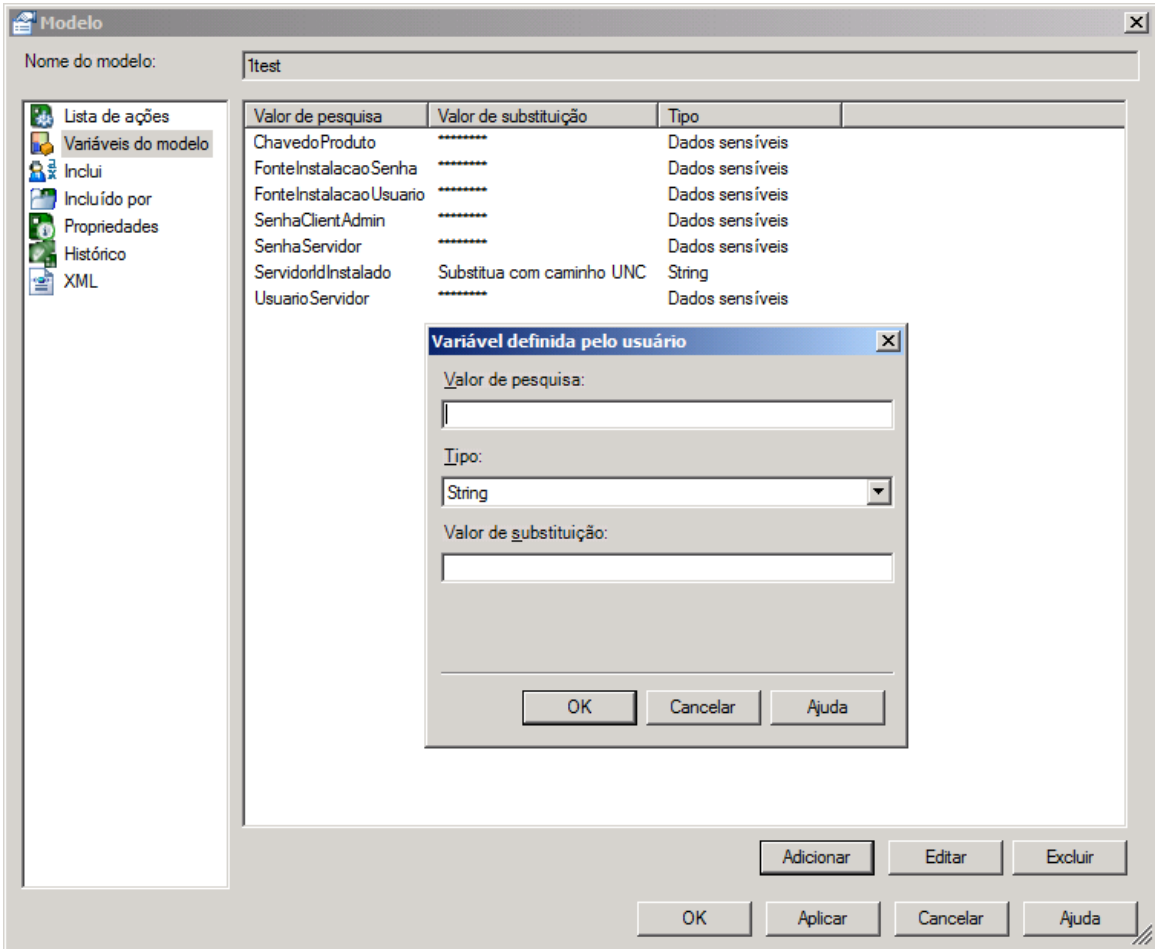
3. Para acrescentar uma variável, clique em **Adicionar**.
4. Digite a variável que deseja adicionar à caixa de texto **Valor de pesquisa** (por exemplo, CoreIP).
5. Digite o valor que deseja substituir na caixa de texto **Valor de substituição** (por exemplo, se o valor da pesquisa for CoreIP, digite o endereço IP com o qual deseja substituir CoreIP).
6. Selecione o tipo.
   - **String:** Digite um valor de string
   - **Valor de banco de dados:** Digite uma string de ID de banco de dados como Computer.Network."NIC Address"
   - **Dados sensíveis:** Digite o valor a ser criptografado no banco de dados.

   Use aspas para os nomes com espaços. A maioria dos valores do banco de dados de inventário pode ser usada.
7. Clique em **OK**.

A consultas ao banco de dados são manipuladas adicionando um prefixo ldbnf: ao Valor de substituição. A tabela do banco de dados e o par de chaves poderão ser usados para procurar uma entrada específica no banco de dados. A variável pública ldDeviceID que é configurada por padrão é um exemplo de como adicionar uma variável de pesquisa de banco de dados.

Definir uma variável de modelo

1. Clique em **Ferramentas > Distribuição > Distribuição de SO**.
2. Em **Modelos de provisionamento**, clique em **Público** ou **Meus modelos** para mostrar uma lista de modelos.
3. Clique duas vezes em um modelo para abrir a tela Modelo.
4. Clique em **Variáveis de modelo**.



5. Clique em **Adicionar**.
6. Digite a variável que deseja adicionar ao campo **Valor de pesquisa**.
7. Digite o valor que deseja substituir no campo **Valor de substituição**
8. Selecione o tipo.

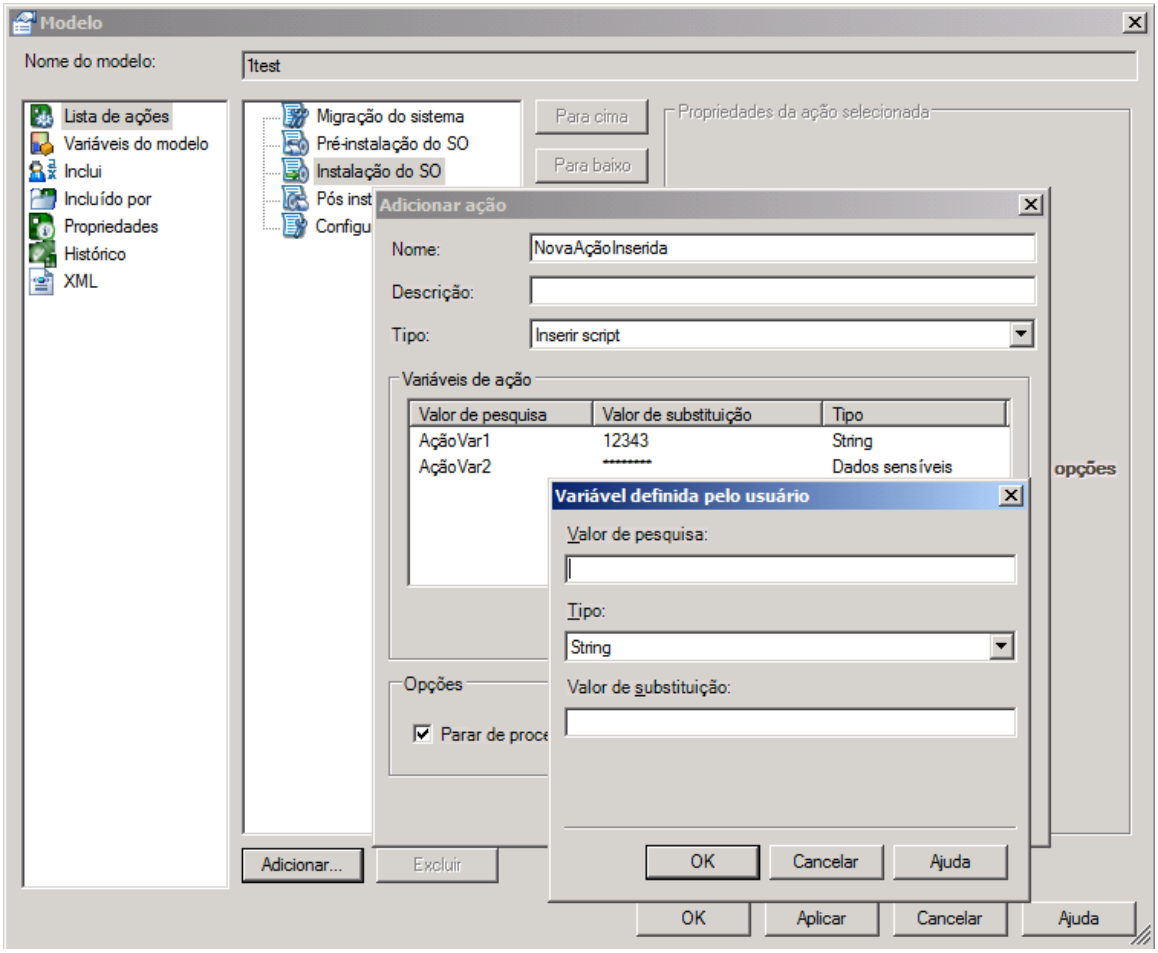
- **String:** Digite um valor de string
- **Valor de banco de dados:** Digite uma string de ID de banco de dados como Computer.Network."NIC Address"
- **Dados sensíveis:** Digite o valor a ser criptografado no banco de dados.

Use aspas para os nomes com espaços. A maioria dos valores do banco de dados de inventário pode ser usada.

9. Clique em **OK**.

Definir uma variável de ação

1. Clique em **Ferramentas > Distribuição > Distribuição de SO**.
2. Clique com o botão direito em um modelo e clique em **Editar**.
3. Clique na **Lista de ações** e selecione uma seção para definir como variável.
4. Clique em **Adicionar** para criar uma nova ação. (Se você quiser modificar uma ação existente, clique com o botão direito na ação e selecione **Propriedades**.)
5. Para acrescentar uma variável de ação, clique em **Adicionar**.



6. Digite a variável que deseja adicionar ao campo **Valor de pesquisa**.

7. Digite o valor que você deseja substituir no campo **Valor de substituição**
8. Selecione o tipo.
   - **String:** Digite um valor de string
   - **Valor de banco de dados:** Digite uma string de ID de banco de dados como Computer.Network."NIC address"
   - **Dados sensíveis:** Digite o valor a ser criptografado no banco de dados.

   Use aspas para os nomes com espaços. A maioria dos valores do banco de dados de inventário pode ser usada.
9. Clique em **OK**.

Criar identificadores exclusivos para novos dispositivos

Para criar identificadores exclusivo para novos dispositivos, use uma variável Pública que é baseado no endereço MAC do dispositivo alvo conforme mostrado abaixo:

Variable (Database) =macAddress	Value = Computer.Network."NIC Address"
Variable (String) = Prefix	Value = UT (Valor do usuário como local - Opcional)
Variable (String) = Suffix	Value = XP (Valor do usuário como SO - Opcional)
Variable (String) = ComputerName	Value = %Prefix%%MACaddr%%Suffix%

Em seguida, use a variável ComputerName nos seus arquivos sysprep.inf ou unattend.txt para identificar exclusivamente o novo dispositivo, conforme mostrado no exemplo de código a seguir:

```
[UserData]
ProductKey=%ProductKey%
FullName="Engineering"
OrgName="LANDesk"
ComputerName=%ComputerName%
```

Tópicos relacionados

"Provisionamento de variáveis de modelo" na página 439

"Definir uma variável públicas (global)" na página 440

Modelos incluídos

A tela Modelo mostra os modelos incluídos no modelo atual (os modelos incluídos também são chamados de modelos filho). Você pode ver modelos inclusos e adicionar modelos ao modelo atual. Quando um modelo é incluído com outro modelo, ele se torna parte do modelo pai. Se você alterar o modelo incluído em sua forma original independente, ele também é alterado no pacote do modelo pai.

Para incluir um modelo, seu ambiente de inicialização e SO alvo precisam corresponder às configurações do modelo pai.

Para adicionar um modelo ao modelo atual

1. Clique em **Ferramentas > Distribuição > Distribuição de SO**.
2. Em **Modelos de provisionamento**, clique em **Público** ou **Meus modelos** para mostrar os modelos.
3. Clique duas vezes em um modelo.
4. Na tela Modelo, clique em **Inclui**.
5. Clique no botão **Incluir**.
6. Usando a estrutura da árvore, vá para o modelo que deseja incluir, selecione-o e clique em **OK**.

A seção **Informações do modelo** exibe detalhes sobre o modelo que deve ser usado na decisão de incluir, ou não, o modelo.

Para excluir um modelo da lista de modelos incluídos, clique em **Remover** para remover o modelo selecionado.

Não aplicável é tratado como curinga.

Modelos pai

A tela **Incluído por** mostra uma lista dos outros modelos que incluem o modelo atual (modelos que incluem o modelo atual são também conhecidos como modelos pai).

Para ver a lista dos modelos que incluem o modelo atual

1. Clique em **Ferramentas > Distribuição > Distribuição de SO**.
2. Em **Modelos de provisionamento**, clique em **Público** ou **Meus modelos** para mostrar os modelos.
3. Clique duas vezes em um modelo.
4. Clique em **Incluído por**.

Adicionar ações a um modelo de provisionamento

Use a caixa de diálogo **Adicionar ação** para criar novas ações de modelos de provisionamento ou para editar as ações de modelos existentes. Os modelos públicos são visíveis à todos os usuários. Os modelos no grupo Meus modelos não são visíveis a todos os usuários e só podem ser modificados pelo criador do modelo ou por usuários com direitos administrativos.

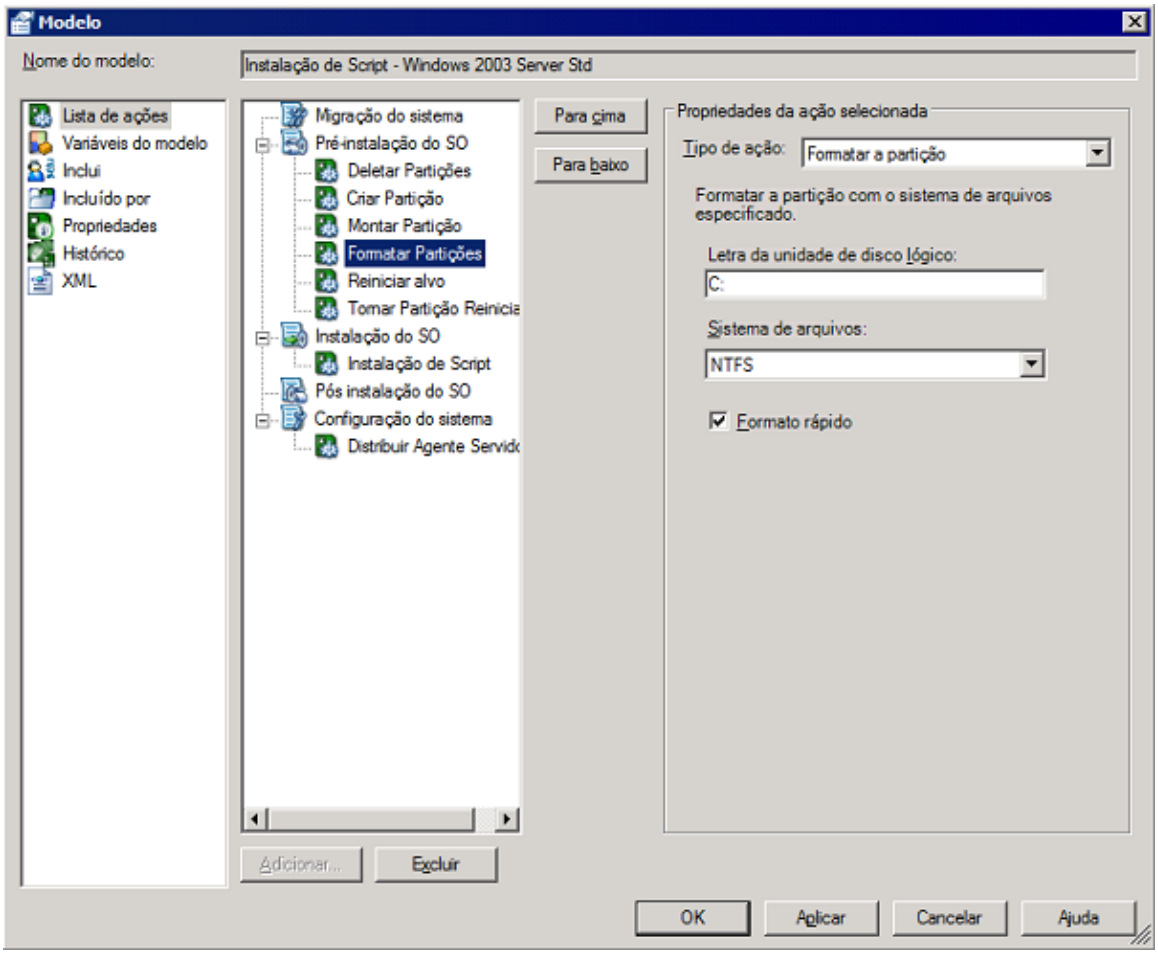
Ações são ordenadas em cinco seções. Você só pode selecionar ações em cada seção aplicável à seção (por exemplo, não é possível selecionar Distribuição de software como uma ação para a seção de Pré-instalação). Você pode adicionar qualquer ação disponível a qualquer seção. No entanto, esteja ciente que algumas ações danificarão o modelo ou poderão causar danos ao seu sistema, tornando-o inútil, se completadas em etapas incorretas.

O botão **Condensar** da barra de ferramentas faz sobrescrever o modelo pai atual para incorporar todos os modelos incluídos de modo que todas as ações dos modelos incluídos façam parte do modelo pai. Isso significa que o modelo pai não tem mais dependências. Isso é útil para a exportação de modelos ou para tornar os modelos públicos. Uma vez que um modelo é condensado, ele é um novo modelo. Não é possível expandir um modelo condensado.

Para adicionar ações a um modelo

1. Clique em **Ferramentas > Distribuição > Distribuição de SO**.
2. Em **Modelos de provisionamento**, clique em **Público** ou **Meus modelos** para mostrar os modelos.

3. Clique duas vezes em um modelo.



4. Na tela Modelo, clique em **Lista de ações**.
5. Clique na seção à qual deseja adicionar uma ação. As seguintes seções estão disponíveis:

   - **Migração do sistema:** Recursos e componentes que precisem ser salvos antes de modificar o sistema (ou migrar um dispositivo para outro hardware ou máquina virtual). Por exemplo, esta seção pode incluir uma ação para capturar informações de perfil quando migrar para o Windows Vista.
   - **Pré-instalação do SO:** Ações que são realizadas quando o dispositivo inicializa no ambiente de pré-instalação (Windows PE). Por exemplo, em um servidor você adicionaria a configuração de RAID nesta seção.
   - **Instalação do SO:** Ações realizadas no ambiente de pré-instalação (Windows PE) quando o SO está instalado.
   - **Pós instalação do SO:** Ações que são realizadas no sistema operacional alvo após ele ter sido instalado, como a execução de uma tarefa de gerenciamento de patch.
   - **Configuração do sistema:** Instalação/execução adicional de aplicativo e configuração do sistema no SO instalado. Por exemplo, adicionar tarefas de instalação de driver nesta seção.

6. Clique em **Adicionar**.
7. Digite um nome específico para a ação no campo **Nome**.
8. Digite uma descrição detalhada da ação no campo **Descrição**.
9. Selecione um tipo de ação na lista **Tipo**. O tipo que você selecionar determinará as opções que precisará especificar para a ação.
10. Se quiser adicionar uma variável que se aplique a essa ação apenas, clique em **Adicionar** em **Variáveis de ação**. Digite o nome e o valor da variável nas caixas de texto e clique em **Salvar**.
11. Selecione **Parar de processar o modelo se esta ação falha** se quiser definir esta ação como essencial para a tarefa de provisionamento. Se a ação pode ser ignorada, limpe esta caixa de texto.
12. Ao concluir, clique em **OK**.

Tipos de ação de provisionamento de modelo

A tabela a seguir mostra os tipos de ações e onde elas se encaixam nas seções por padrão. Você pode adicionar qualquer tipo de ação a qualquer seção. Observe, porém, que algumas seções cabem inerentemente em determinadas seqüências no provisionamento. Se uma ação é executada fora da sua seqüência destinada, pode haver conseqüências indesejáveis.

Nome da ação	Migração do sistema	Pré-instalação do SO	Instalação do SO	Pós instalação do SO	Configuração do sistema
Capturar imagem			X		
Capturar perfil	X				
Configurar agente					X
Configurar SO alvo				X	
Controlar serviço					X
Copiar arquivo	X	X	X	X	X
Criar diretório	X	X	X	X	X
Excluir arquivo	X	X	X	X	X
Distribuir imagem			X		
Distribuir perfil					X
Distribuir software					X
Fazer download do arquivo	X	X	X	X	X
Faça do	X	X	X	X	X

Nome da ação	Migração do sistema	Pré-instalação do SO	Instalação do SO	Pós instalação do SO	Configuração do sistema
download do servidor preferencial					
Executar arquivo	X	X	X	X	X
Geração de imagem independente de hardware				X	
Injetar script	X	X	X	X	X
Instalar serviço					X
Unir domínio					X
Mapear/des-conectar unidade	X	X	X	X	X
Mapear/Des-mapear a unidade no servidor preferencial	X	X	X	X	X
Partição		X	X	X	
Corrigir sistema					X
Rein-icializar/desligar	X	X	X	X	X
Substituir texto	X	X	X	X	X
Instalação por script			X		
Desinstalar serviço					X
Descompactar arquivo	X	X	X	X	X
Atualizar registro					X
Aguardar	X	X	X	X	X

Capturar imagem (somente a seção de instalação do SO)

A ação Capturar imagem permite a captura de uma imagem durante a instalação do SO através do uso da ferramenta de imagem especificada. Se a ferramenta ou o conteúdo a ser capturado em uma imagem estiver em um compartilhamento, será necessário incluir a ação Mapear unidade antes da ação Capturar imagem para autenticar no compartilhamento.

- **Selecione o tipo de imagem:** Selecione o tipo de imagem que você quer capturar. Se você selecionar a Symantec ou outro, você também deverá fornecer o caminho do aplicativo usado para imagens.
- **Especifique o caminho UNC do arquivo de imagem**: Insira um caminho UNC da imagem capturada, inclusive o nome do arquivo. Configure seu servidor preferencial com credenciais válidas para a parte do caminho de arquivo de imagem. Esta opção é usada quando você seleciona ou LANDesk ImageW ou ImageX como o tipo de imagem.
- **Especifica o caminho mapeado da unidade para o arquivo de imagem**: Insira um caminho para o arquivo de imagem, incluindo uma letra e o nome do arquivo de imagem. Esta opção é usada quando você seleciona Symantec ou outro como o tipo de imagem.
- **Especifica o caminho mapeado da unidade para a ferramenta de imagem**: Insira um caminho mapeado para a unidade e o nome do arquivo para o aplicativo de imagens. Esta opção é usada quando você seleciona Symantec ou outro como o tipo de imagem.
- **Parâmetros da linha de comando:** insira parâmetros da linha de comando para personalizar a forma como a imagem é capturada.
- **Validar:** Clique este botão para gerar uma linha padrão de comando para a ferramenta de imagens e caminho que você especificou. Você pode adicionar outros parâmetros de linha de comando depois de clicar em Validar, mas se você já inseriu qualquer parâmetro personalizado, eles serão removidos quando você clicar em Validar.

NOTA: Para evitar o problema do sistema de arquivos travar aberto no WinPE, primeiro é necessário executar o Sysprep da sua imagem. No Windows Vista, siga as etapas abaixo.

1. Inicie o Vista.
2. Altere para o diretório %SystemRoot%\System32\sysprep.
3. Execute "sysprep /generalize /shutdown".
4. Inicie o PE e execute ImageX.

As etapas do Windows XP/2003 não requerem a mudança de /generalize e /shutdown para o sysprep. A mudança de /factory não funcionará nesses sistemas operacionais.

Capturar perfil (somente na seção de migração do sistema)

Esta ação executa o assistente de migração de usuário para capturar um ou mais perfis. Para usar esta ação, você deve saber onde o comando do arquivo XML assistente da migração de usuário que arquivo adjunto de XML de comando é localizado no servidor núcleo e onde os perfis gravados serão armazenados.

Você pode usar identificadores raros para nomear perfis quando eles são salvos ou você pode especificar um nome de arquivo para o perfil.

Para usar o assistente de migração de usuário, dispositivos gerenciados devem ter o agente LANDesk padrão, que inclui o analisador de inventário, agendador local e os agentes de distribuição de softwares. A migração de perfil usa o agente de distribuição de softwares para distribuir arquivos.

- **Selecione o arquivo XML de comando do assistente de migração do usuário:** Especifique a localização do arquivo XML de comando do assistente de migração de usuário gravado no servidor núcleo (geralmente no compartilhamento ldmain, na pasta ldlogon\uma\commandxml). Você pode especificar o caminho e nome de arquivo em UNC ou formato de HTTP. Clique em **Procurar** para localizar o arquivo de comando que você quer usar. Se você quer editar um arquivo existente de comando ou cria um novo, clique **Editar**. Selecione um arquivo e clique **Editar**, ou clique **Novo** criar um novo.
- **Caminho UNC para perfis salvos:** Especifique onde gravar os arquivos de perfil. Digite um caminho UNC ou clique em **Procurar** e selecione um caminho. Os perfis podem ser gravados em qualquer servidor/compartilhamento disponível, inclusive no servidor núcleo. Os perfis são gravados com uma extensão .sma.
- **Especifique um nome completo ao invés de usar variáveis:** Selecione esta caixa de seleção se você não quer nomear o perfil usando os identificadores exclusivos.
- **Identificadores exclusivos de nome do arquivo:** Selecione qualquer combinação do nome de computador, endereço de MAC, e número de série para criar o nome de arquivo de cada perfil. (Por exemplo, se você selecionar **Número de série** e o número de série da máquina é 123A567B, o nome de perfil será gravado como "123A567B.sma.")

Configurar agente (somente a seção Configuração do sistema)

A ação Configurar agente lhe permite selecionar uma configuração de agente para instalar no servidor de provisionamento. Essa ação deve ser a primeira coisa a ser feita após a reinicialização que segue a ação de instalação do SO. As configurações são adicionadas à lista suspensa à medida que são criadas na Configuração de agente. Essa ação só pode ser concluída como parte de um modelo que inclui a instalação por script ou ações de distribuição de imagem ou, se a máquina cliente já estiver configurada com um agente.

- **Nome de configuração:** O nome da configuração. Selecione uma configuração da lista de configurações válidas de agente.
- **Insira as credenciais:** Digite o domínio e o nome de usuário para fazer login no servidor núcleo onde o agente de configuração reside.
- **Use uma variável para a senha:** Selecione esta caixa de seleção para usar uma variável para a senha. Essa variável é definida em **Variáveis de modelo** em **Tipo de dados sensíveis**. Insira o nome da variável na caixa de Senha entre sinais de percentagem (%variablename%). Para mais informações, veja "Definir uma variável de modelo" na página 442.
- **Senha:** Digite a senha para fazer login no servidor núcleo. Confirme a senha na caixa **Confirmar senha**.
- **Reinicializar se for necessário:** Selecione esta caixa de seleção para permitir o dispositivo reiniciava depois de configuração de agente, se um reinicia é exigido.

Quando você instala um novo service pack, os IDs do banco de dados de configuração do agente são mudados. Isso significa que os modelos que fazem referência a essas configurações se tornam desatualizados. Como resultado, qualquer histórico de provisionamento que faça referência a essas configurações será incapaz de exibir o nome da configuração ao qual fez referência. Qualquer modelo que faça referência às configurações antigas deverá ser atualizado para que possa ser executado corretamente. O nome da configuração não é exibido na página Histórico e, se você tentar reagendar este modelo, ele falhará na ação Configurar agente devido a esse problema. Para corrigi-lo, você deverá clonar o modelo, abrir o modelo clonado, abrir a ação Configuração de agente e atribuir a configuração que deseja usar. Assim a tarefa será executada com êxito.

Configurar SO alvo (somente a seção pós-instalação de SO)

Essa ação insere o agente de provisionamento (ldprovision) em uma imagem, assim o agente pode ser instalado depois da reinicialização. Ela é necessária para o provisionamento contínuo após o início do sistema operacional. Para que esta ação funcione, as seguintes condições deverão ser atendidas:

1. A unidade de sistema do Windows precisa ser montada.
2. O sistema de arquivos do Windows precisa ser sysprepped ou ter um agente no computador
3. O Linux não pode ter nenhum sistema de arquivos incomuns (xfs, jfs, bobfs). Os sistemas reiserfs e ext2/3 são os únicos com suporte.
4. O sistema raiz do Linux não pode estar em um controlador de RAID de software ou em um RAID de software (md). Configurações de RAID de hardware reais são permitidas, desde que o driver do controlador seja reconhecido pelo PE.

- **Inserir ID exclusivo:** Para usar o ID de dispositivo, selecione esta caixa de verificação e digite o ID do dispositivo na caixa de texto.

Essa ação deve ser a última executada na seção de pós-instalação do SO, porque inclui uma operação de reinicialização.

Controlar serviço (somente a seção de Configuração do sistema)

A ação de Serviço de controle inicia, interrompe ou reinicializa um serviço específico. Para essa ação, o SO alvo deve ser Windows.

- **Nome do serviço:** O nome de exibição do serviço.
- **Ação do controle de serviço:** A ação que executará o serviço. Ela pode ser Parar, Iniciar ou Reiniciar.

Copiar arquivo (todas as seções)

A ação Copiar arquivo copia arquivos para locais específicos no servidor alvo. A origem e o destino podem estar em um compartilhamento. Se assim for, será necessário incluir uma ação de Mapear unidade antes da ação Copiar arquivo. A ação Copiar arquivo pode ser recursiva, o que significa que todos os arquivos/pastas abaixo do caminho de origem podem ser copiados, mantendo sua estrutura original. Suporta caracteres curingas (como *.exe ou ld*.*).

- **Caminho fonte e nome de arquivo:** o caminho do servidor/compartilhamento e o local do nome de arquivo a ser copiado. Caso deseje copiar todos os arquivos e pastas abaixo do caminho de origem, não há necessidade de colocar um nome de arquivo.

- **Caminho de destino e nome de arquivo:** O local do nome de arquivo e o caminho do servidor/compartilhamento onde o arquivo será copiado.
- **Copiar subdiretórios:** Copia todas as subpastas e arquivos abaixo da origem.

Criar diretório (todas as seções)

A ação Criar diretório cria um diretório no local especificado e pode criar o diretório pai, se necessário.

- **Caminho do diretório:** Digite o caminho do diretório a ser criado.
- **Criar diretório pai se necessário:** Selecione esta caixa de seleção para criar o diretório pai.

Excluir arquivo (todas as seções)

Essa ação remove arquivos de locais específicos no servidor alvo. O caminho pode estar em um compartilhamento. Se assim for, será necessário incluir uma ação de Mapear unidade antes da ação Excluir arquivo. A ação Excluir arquivo pode ser recursiva, o que significa que todos os arquivos/pastas abaixo do caminho de origem podem ser excluídos. Suporta caracteres curingas (como *.exe ou ld*.*).

- **Caminho e nome de arquivo:** insira o caminho completo e o nome do arquivo a ser excluído.
- **Excluir subdiretórios:** Apaga todas as subpastas e arquivos abaixo da origem.

Distribuir imagem (somente a seção de instalação do SO)

Essa ação distribui a imagem selecionada para o servidor alvo através da ferramenta de imagem especificada. Se a ferramenta ou a imagem a ser distribuída estiver em um compartilhamento, será necessário colocar a ação Mapear unidade antes da ação Distribuir imagem para autenticar no compartilhamento.

É necessário reinicializar manualmente após a distribuição de uma imagem

- **Selecione o tipo de imagem:** Selecione o tipo de imagem que deseja distribuir. Se você selecionar a Symantec ou outro, você também deverá fornecer o caminho do aplicativo usado para imagens.
- **Especifique o caminho UNC do arquivo de imagem**: Insira um caminho de UNC à imagem distribuída, inclusive o nome do arquivo de imagem. Configure seu servidor preferencial com credenciais válidas para a parte do caminho de arquivo de imagem. Esta opção é usada quando você seleciona ou LANDesk ImageW ou ImageX como o tipo de imagem.
- **Especifica o caminho mapeado da unidade para o arquivo de imagem**: Insira um caminho para a imagem, inclusive uma letra para a unidade e o nome do arquivo de imagem. Esta opção é usada quando você seleciona Symantec ou outro como o tipo de imagem.
- **Especifica o caminho mapeado da unidade para a ferramenta de imagem**: Insira um caminho mapeado para a unidade e o nome do arquivo para o aplicativo de imagens. Esta opção é usada quando você seleciona Symantec ou outro como o tipo de imagem.
- **Parâmetros da linha de comando:** Insira parâmetros de linha de comando para personalizar a forma como a imagem é distribuída.
- **Validar:** Clique este botão para gerar uma linha padrão de comando para a ferramenta de imagens e caminho que você especificou. Você pode adicionar outros parâmetros de linha de comando depois de clicar em Validar, mas se você já inseriu qualquer parâmetro personalizado, eles serão removidos quando você clicar em Validar.

Distribua o perfil (somente na seção de configuração de sistema)

Esta ação executa o assistente de migração de usuário para distribuir um ou mais perfis que foram capturados e gravados. Para usar esta ação, você deve saber onde perfis gravados foram armazenados.

Para usar o assistente de migração de usuário, dispositivos gerenciados devem ter o agente LANDesk padrão, que inclui o analisador de inventário, agendador local e os agentes de distribuição de softwares. A migração de perfil usa o agente de distribuição de softwares para distribuir arquivos.

- **Caminho do UNC onde o perfil previamente foi gravado:** Especifique onde os arquivos de perfil são gravados. Digite um caminho UNC ou clique em **Procurar** e selecione um caminho. Os perfis podem ser gravados em qualquer servidor/compartilhamento disponível, inclusive no servidor núcleo. Os perfis são gravados com uma extensão .sma.
- **Especifique um nome completo ao invés de usar variáveis:** Selecione esta caixa de seleção se você não quer nomear o perfil usando os identificadores exclusivos.
- **Identificadores exclusivos de nome do arquivo:** Selecione qualquer combinação do nome de computador, endereço de MAC, e número de série para criar o nome de arquivo de cada perfil. (Por exemplo, se você selecionar **Número de série** e o número de série da máquina é 123A567B, o nome de perfil será gravado como "123A567B.sma.")

Distribuir software (somente seção de Configuração do sistema)

Essa ação distribui um pacote de distribuição de software para o alvo. Você pode escolher qualquer pacote de distribuição que tiver salvo na ferramenta Pacotes de distribuição. Esta ação somente poderá ser concluída após a ação de configuração de agentes ou após os agentes terem sido instalados no dispositivo.

- **Pacote de distribuição de software:** selecione o pacote que deseja distribuir.

Descarregar arquivo (todas as seções)

A ação Descarregar arquivo faz o download do arquivo selecionado usando um usuário anônimo (login anônimo no HTTP) em um destino especificado. Se os arquivos a serem descarregados ou o destino estiverem em um compartilhamento, será necessário posicionar a ação Mapear unidade antes da ação Descarregar arquivo para autenticar no compartilhamento.

- **Caminho fonte e nome de arquivo:** o caminho do servidor/compartilhamento atual e o nome do arquivo a ser descarregado. O descarregamento de arquivos de um caminho UNC não é suportado. Caso deseje descarregar um arquivo de um caminho UNC, é necessário usar a ação Mapear unidade para mapear o caminho UND e depois usar a ação Copiar arquivo.
- **Caminho de destino e nome de arquivo:** o local onde o arquivo será descarregado.
- **Usar servidor proxy:** habilita a opção de servidor proxy para descarregar um arquivo. Por padrão, esta opção é desativada. Se você habilitar um servidor proxy, deverá preencher os campos de endereço e porta abaixo.
- **Endereço:** Identifica o endereço IP do servidor proxy.
- **Porta:** Identifica o número de porta do servidor proxy.
- **Requer login:** Permite digitar um nome de usuário e uma senha se o servidor proxy usa credenciais em vez de ser um servidor proxy transparente.
    - **Nome de usuário:** Insira um nome válido de usuário com credenciais de autenticação ao servidor de procurador.

- **Use uma variável para a senha:** Selecione esta caixa de seleção para usar uma variável para a senha. Essa variável é definida em **Variáveis de modelo** em **Tipo de dados sensíveis**. Insira o nome da variável na caixa de Senha entre sinais de percentagem (%variablename%). Para mais informações, veja "Definir uma variável de modelo" na página 442.
- **Senha:** Digite a senha do usuário. Confirme a senha na caixa **Confirmar senha**.

Faça do download do servidor preferencial (todas as seções)

Esta ação usa replicação de conteúdo para fazer o download de um servidor preferencial ao dispositivo de alvo. O download pode ser um único arquivo ou o conteúdo de uma pasta (inclusive subpastas) no servidor de fonte. Para usar esta ação, você deve ter configurado ao menos um servidor preferencial usando a ferramenta Contente de replicação. A escolha de qual servidor preferencial é usada de acordo com as configurações que você fez quando você monta servidores preferidos na ferramenta Replicação de conteúdo.

- **Origem**: Especifique o caminho ao arquivo ou pasta que você quer fazer o download. Este caminho deve existir em todos os compartilhamentos usados para downloads de servidores preferenciais.
- **Diretório de download:Selecione esta caixa de seleção para fazer o download a pasta inteira especificada na caixa de Origem.** Se estiver vazio, somente o arquivo que você especificar será baixado.
- **Destino:** Especifique o caminho no dispositivo de alvo a que você quer copiar o arquivo ou pasta.
- **Locais preferenciais de download:** As três caixas de seleção permite que você especifique quais origens de download você quer usar. Eles são listados na ordem de prioridade: se todos três caixas são selecionadas, um download de igual é tentado primeiro, seguido por um servidor preferencial, e finalmente um download de fonte.
    - **Tentar par:** Selecione esta caixa de seleção para tentar o download de par. **O replicador verificará primeiro os pares locais para arquivos de origem que estão sendo duplicados.** Se o replicador não pode achar os arquivos num par, então tentará receber o arquivo de um servidor preferencial nem o servidor de fonte. Esta opção pode reduzir a carga de trânsito em preferido e servidores de fonte.
    - **Tentar servidor preferencial:** Selecione esta caixa de seleção para fazer o download de um servidor preferencial. Se o replicador não pode achar o arquivo num servidor preferencial, então tentará receber o arquivo do servidor de fonte.
    - **Permitir fonte:** Selecione esta caixa de seleção para fazer o download da arquivo de origem. Isto é recomendado somente como uma opção secundária se um download de par de servidor preferencial não for concluído.
- **Largura de banda usada do núcleo ou do servidor preferencial:** Ajusta a prioridade desta tarefa específica acima de outro tráfego de rede. Quanto mais alta for a porcentagem do deslizador, maior será a quantidade de largura de banda usada por esta tarefa acima de qualquer outro tráfego. As conexões WAN em geral são mais lentas, por isso recomenda-se com frequência colocar este deslizador na porcentagem mais baixa.
- **Largura de banda usada ponto-a-ponto:** Ajusta a prioridade desta tarefa específica acima de outro tráfego de rede. Quanto mais alta for a porcentagem do deslizador, maior será a quantidade de largura de banda usada por esta tarefa acima de qualquer outro tráfego. As conexões de LAN são, em geral, mais rápidas que as conexões WAN, por isso recomendada-se frequentemente que o slider seja definido em uma porcentagem mais alta que a WAN.

Executar arquivo (todas as seções)

A ação Executar arquivo executa o arquivo selecionado no servidor alvo, com quaisquer parâmetros de linha de comando ou códigos de retorno que você especificar.

- **Caminho alvo e nome de arquivo:** o local do arquivo que deseja executar.
- **Parâmetros da linha de comando:** Insira um parâmetro de linha de comando para personalizar a forma como o arquivo é executado.
- **Diretório de trabalho:** O programa será executado com referência a esse diretório. Qualquer arquivo de suporte do programa deve residir nesse diretório. Os parâmetros de linha de comando iniciam nesse ponto de referência.
- **Valor de retorno esperado:** o valor de retorno do aplicativo esperado na execução. Ele pode ser Qualquer, Igual (=), Inferior a (<), Superior a (>) ou Entre. Se o valor for diferente de Qualquer, insira os valores esperados nas caixas fornecidas.
- **Inserir:** Abre a caixa de diálogo **Variável de ambiente**, onde é possível acrescentar uma variável de ambiente e seu valor.
    - **Nome:** Digite o nome da variável de ambiente do arquivo. Use o sinal de porcentagem duplo para especificar variáveis de ambiente (por exemplo, %%windir%%\system32\calc.exe).
    - **Valor:** insira o valor da variável.
- **Modificar:** modifique a variável selecionada.
- **Remover:** exclua a variável selecionada.
- **Capturar a saída de comando:** Quando esta caixa de seleção é selecionada, saída do executável é escrito em um arquivo de log. Limpe a caixa de seleção para evitar capturar a saída.

Imagens independentes de hardware (apenas pós-instalação de SO)

A ação de imagem independente de hardware inclui a ferramenta de imagem independente de hardware (hiiclient.exe) no processo de provisinamento. Geração de imagem independente de hardware (HII) permite que você crie um único repositório de drivers de dispositivo que podem ser injetados em modelos de provisionamento ou scripts de distribuição. É instalada uma imagem básica no dispositivo e a ferramenta HII, então, injeta drivers que são específicos ao modelo de dispositivo.

Esta ação só é inclusa na seção Pós-instalação do SO para modelos baseados no ambiente de pré-inicialização do Windows. Após o SO ser instalado, mas antes do dispositivo reinicializar, a ferramenta HII detecta o modelo do dispositivo e obtém os drivers para o modelo. Os drivers são instalados no dispositivo e suas informações são incluídas no registro. Após a reinicialização, quando o SO inicia, ele configura os drivers.

- **Usar UNC fazer o download arquivos de driver:** selecione esta caixa de seleção para especificar que somente um UNC é usado para acessar o repositório de HII.

Se você usar esta ação, inclua uma ação Reinicializar após a mesma na seção Pós-instalação de SO.

Injetar script (todas as seções)

Essa ação injeta um script no sistema de arquivo alvo do SO. Por exemplo, você pode injetar o sysprep.inf na ação Distribuir imagem ou unattend.txt em uma instalação com Script. Os scripts que você pode selecionar são os presentes na lista **Instalar scripts** (acessada através do botão **Instalar scripts** na barra de ferramentas de Provisionamento) que pode ser aplicado ao modelo atual.

Injetar um script copia o arquivo para a máquina local e também substitui variáveis dentro do arquivo. Esta ação é útil quando você quer substituir variáveis em qualquer arquivo de texto, tal como um arquivo de resposta de Sysprep de Windows.

- **Nome do script:** o nome do script.
- **Nome do arquivo alvo:** o local do script que deseja injetar.

Instalar serviço (somente a seção de Configuração do sistema)

Para essa ação, o SO alvo deve ser Windows.

- **Nome de exibição:** o nome que você deseja exibir para representar o serviço.
- **Nome do serviço:** o nome do serviço.
- **Descrição do serviço**: Uma descrição do serviço
- **Caminho alvo e nome de arquivo:** O local do serviço que você deseja instalar.
- **Parâmetros da linha de comando:** Insira qualquer parâmetro da linha de comando que personalizará a forma como o serviço é instalado.
- **Tipo de inicialização do serviço:** pode ser Manual, Automática ou Desativada.
- **Serviço interativo:** Selecione esta opção para ser mostrada na área de trabalho ou em qualquer interface do usuário que possa ser usada pelo usuário conectado quando o serviço é iniciado. Isso inclui caixas de mensagem que o serviço pode chamar durante o processo de instalação. Se esta caixa de seleção não for selecionada, o modelo será executado sem interação com o usuário e assumirá as seleções padrão de qualquer serviço de mensagens. Se o serviço exibir qualquer message durante a inicialização, o modelo poderá ser pausado até que a caixa de diálogo da mensagem seja fechada.

Unir domínio (somente a seção Configuração do sistema)

Une o dispositivo alvo a um domínio ou grupo de trabalho.

- **Selecionar tipo de operação:** Pode ser Unir domínio ou Unir grupo de trabalho.
- **Nome do domínio:** Digite o domínio a unir.
- **Nome do grupo de trabalho:** Digite o grupo de trabalho que deseja unir.
- **Nome de usuário:** Digite o nome de usuário necessário para autenticação no domínio.
- **Use uma variável para a senha:** Selecione esta caixa de seleção para usar uma variável para a senha. Essa variável é definida em **Variáveis de modelo** em **Tipo de dados sensíveis**. Insira o nome da variável na caixa de Senha entre sinais de percentagem (%variablename%). Para mais informações, veja "Definir uma variável de modelo" na página 442.
- **Senha:** Insira a senha correspondente ao nome do usuário acima. Confirme a senha na caixa **Confirmar senha**.

Mapear/desconectar unidade (todas as seções)

Use esta ação para mapear ou desmapear (desconectar) uma unidade em dispositivos de Windows, ou para dispositivos Linux, para conectar ou desconectar um recurso. Alguns sistemas não aceitam mapeamentos de unidade abaixo de H.

- **Mapear/desmapear unidade:** Selecione se esta ação é para mapear ou desmapear (desconectar) uma unidade, ou ligar ou desconectar um recurso (dispositivos de Linux).
- **Caminho UNC:** insira o servidor e compartilhamento para onde deseja mapear.

- **Caminho do recursos para desconectar**: Ao desconectar um recurso, especifique o caminho ser desconectado.
- **Letra da unidade/Ponto de montagem:** Insira a letra da unidade para a qual você quer mapear. Se você decidir desmapear uma unidade, digite o nome da unidade que deseja desconectar. No Linux, especifique o ponto de montagem em que o recurso ou filesystem é montado.
- **Nome de usuário:** Insira o nome da credencial do usuário para fazer login na unidade.
- **Use variáveis para a senha:** Selecione esta caixa de seleção para usar uma variável para a senha. Essa variável é definida em **Variáveis de modelo** em **Tipo de dados sensíveis**. Insira o nome da variável na caixa de Senha entre sinais de percentagem (%variablename%). Para mais informações, veja "Definir uma variável de modelo" na página 442.
- **Senha:** Insira a senha correspondente ao nome do usuário acima. Confirme a senha na caixa **Confirmar senha**.

Mapear/Desmapear unidade ao servidor preferencial (todas as seções)

Esta ação mapeia uma unidade no dispositivo alvo para um caminho em um servidor preferencial (ou o servidor de fonte). O impulso traçando estadas em efeito até que o impulso é explicitamente não-mapeado (desconectado), então você deve incluir uma ação de Desmapeamento em um modelo depois de que uma ação que faz o download de um servidor preferencial. Para usar esta ação, você deve ter configurado ao menos um servidor preferencial usando a ferramenta Contente de replicação. A escolha de qual servidor preferencial é usada de acordo com as configurações que você fez quando você monta servidores preferidos na ferramenta Replicação de conteúdo.

- **Letra da unidade:** Insira a letra da unidade para a qual você quer mapear. Se você decidir desmapear uma unidade, digite o nome da unidade que deseja desconectar.
- **Desmapear unidade:** Selecione esta caixa de seleção se a ação for desmapear uma unidade. A ação irá simplesmente desmapear (desconectar) a unidade especificada na letra da Unidade.
- **Caminho:** Insira o caminho da unidade no formato de UNC (\\sharename\path). Este caminho deve existir no servidor de origem em todos os compartilhamentos usados para downloads de servidores preferenciais.
- **Tentar servidor preferencial:** Selecione esta caixa de seleção na primeira tentativa de mapear a unidade ao servidor preferencial mais próximo que contém a estrutura da pasta específica. Se nenhum servidor preferencial for encontrado com a estrutura de pasta, uma tentativa será feita para mapear a unidade ao caminho no servidor de origem.
- **Requer servidor preferencial:** Selecione esta caixa de seleção para mapear a unidade ao servidor preferencial mais próximo que contém a estrutura da pasta específica. Se nenhum servidor preferencial for encontrado com a estrutura de pasta, a tarefa falha (antes que mapa ao servidor de fonte).
- **Não permitir servidor preferencial:** Selecione esta caixa de seleção para traçar o impulso ao caminho no servidor de fonte, sem traçar a um servidor preferencial.

Particionar (somente para seções de pré-instalação de SO, instalação de SO, pós-instalação de SO)

A ação Partição permite completar uma variedade de ações em relação a partições no servidor alvo. Selecione ações da partição na lista Tipo de ação. As ações são as seguintes:

NOTA: O ambiente de inicialização e o SO alvo precisam ser definidos antes da execução desta ação.

Criar partição: Crie uma partição no disco especificado.

- **Disco:** Digite a ID do disco. No Windows, é o número do disco. No Linux, é o nome do disco.
- **Tipo de partição:** selecione o tipo de partição. Uma partição pode ser Primária, Estendida ou Lógica.
- **Tamanho:** O tamanho da partição a ser criada, em MB.
- **Offset:** um número (no formato byte de 8 bits) que indica a profundidade, no disco, onde deverá ser criada a partição.
- **Iniciar:** A posição de início da partição (número do cilindro).
- **Fim:** A posição de término da partição (número do cilindro).

Remover partição: exclua uma partição no disco especificado.

- **Remover do disco:** Digite a ID do disco. No Windows, é o número do disco. No Linux, é o nome do disco.
- **ID de partição:** o número da partição a ser removida.

Remover todas as partições: exclui todas as partições do disco.

- **Remover do disco:** Digite a ID do disco. No Windows, é o número do disco. No Linux, é o nome do disco.

Formatar partição: cria uma estrutura de sistema de arquivos em uma partição.

- **Letra de unidade do disco lógico:** A letra da unidade da partição a ser formatada (Windows).
- **Partição:** O nome do dispositivo da partição a ser formatada (Linux).
- **Sistema de arquivos:** No Windows, os sistemas de arquivo são FAT, FAT32 e NTFS. Para Linux, os sistemas de arquivo são ext2, ext3, reiserfs e linux-swap.
- **Formatação rápida:** Selecione essa caixa de seleção para executar uma formatação rápida na partição.

Montar partição: monta uma partição.

- **Disco:** O número do disco a ser montado (Windows).
- **Partição:** O nome do dispositivo da partição (Linux).
- **ID de partição:** O número da partição a ser montada (Windows).
- **Sistema de arquivos:** Para Linux, os sistemas de arquivo são ext2, ext3, reiserfs e linux-swap.
- **Caminho do arquivo a montar:** O nome da partição a ser montada. O ponto de montagem deve existir (Linux).
- **Letra de unidade do disco lógico a criar:** A letra da unidade da partição a ser montada (Windows).

Desmontar partição: desmonta uma partição.

- **Disco:** o número do disco a ser desmontado.
- **ID de partição:** no Windows, o número da partição a ser desmontada. No Linux, o nome do dispositivo da partição.
- **Letra de unidade do disco lógico a remover:** A letra da unidade da partição a ser desmontada (Windows).

- **Ponto de montagem a ser desmontado:** O nome da partição a ser desmontada (Linux). O ponto de montagem deve existir.

Tornar inicializável: Tornar uma partição inicializável.

- **Disco:** O número do disco que será inicializável. No Windows, é o número do disco. No Linux, é o nome do disco.
- **ID de partição:** o número da partição a ser tornada inicializável.
- **Inicializável:** Selecione a caixa de seleção para tornar a partição inicializável.
- **Windows 7/Windows 2008 R2 com uma partição de sistema separada:** Selecione esta caixa de seleção para criar uma partição de SO separada.
- **ID da partição do SO:** O número da partição separada de SO.

Expandir partição: Expande a última partição da unidade. Deve haver espaço livre.

- **Disco:** o número do disco a ser montado.
- **ID de partição:** no Windows, o número da partição a ser montada. No Linux, o nome do dispositivo da partição.
- **Tamanho:** O novo tamanho da partição em MB (Windows). Caso fique em branco, a partição será expandida até preencher o disco.
- **Iniciar:** A posição de início da partição (número do cilindro).
- **Fim:** A posição de término da partição (número do cilindro).

Corrigir sistema (somente a seção de Configuração do sistema)

A ação Corrigir sistema analisa se o dispositivo alvo tem vulnerabilidades e as corrige. Esta ação só poderá ser executada depois que a ação Configuração (que instala o agente de atualizações de software) for executada.

- **Analisar somente:** analisa a máquina para verificar vulnerabilidades.
- **Analisar e reparar vulnerabilidade:** analisa a máquina para verificar vulnerabilidades e, onde possível, as repara.
- **Analisar e reparar grupo:** analisa a máquina para verificar vulnerabilidades e repara as vulnerabilidades incluídas no grupo.
- **ID da vulnerabilidade:** um ID de vulnerabilidade válido do Patch Manager. Se o ID não for válido, a ação falhará.
- **ID do grupo:** um ID de grupo válido do Patch Manager. Se o ID não for válido, a ação falhará. Você pode clicar no botão da lista de ID de grupo para selecionar um grupo de vulnerabilidade que tiver criado.

As definições de vulnerabilidade núcleo devem ser atualizadas antes da execução dessa ação. Todos os patches a serem reparados devem ser descarregados no núcleo antes da execução de qualquer opção de remediação nesta ação.

Reinicializar/Desligar (todas as seções)

Reinicializa ou desliga o servidor. Uma reinicialização deve acontecer logo após a ação de instalação do SO. Na reinicialização, o agente de provisionamento reinicia o modelo para continuar o progresso das tarefas de provisionamento. Use a ação Reinicializar para mover a seção de migração do sistema para seções do SO ou seções do SO para a seção de configurações do sistema. Suporta várias reinicializações.

- **Reinicialização:** Desliga e reinicializa o servidor.
- **Desligar:** desliga o servidor no final da tarefa de provisionamento e o deixa desligado (off). Você precisa verificar se esta ação é a última ação no modelo, caso contrário outras ações adicionais não serão realizadas.
- **Inicializar para WinPE gerenciado (inicialização virtual):** Inicialize a máquina do cliente em um ambiente WinPE administrado. As ações serão executadas como instruído pelo servidor núcleo. Esta opção é para ser usada quando não houver nenhum servidor PXE na rede para provisionamento.
- **Limite de tempo de confirmação:** Especifique o número de segundos que uma mensagem de confirmação é exibido antes que tempo acabe.

Substituir texto (todas as seções)

Substitui o texto em um arquivo existente.

- **Caminho de origem e nome do arquivo:** o caminho e o nome do arquivo em que o texto será substituído.
- **Localizar:** o texto existente que será substituído.
- **Substituir por:** O texto que substituirá o texto existente.
- **Substituir a primeira ocorrência, Substituir todas as ocorrências:** Substitui o novo texto na primeira vez que ele é encontrado ou sempre que ele for encontrado.

Instalação por script (somente a seção de instalação do SO)

Instala um sistema operacional através do uso de scripts personalizados. Só pode haver uma ação que instala um SO.

Windows

- **Caminho UNC para a fonte da instalação:** Esse é o caminho onde o arquivo executável é encontrado na origem da instalação. Ele deve ter sido montado na seção de Pré-instalação do SO (ação Mapear unidade).
- **Domínio e nome de usuário:** Digite o domínio e o nome de usuário para fazer login no dispositivo onde o executável reside.
- **Use variáveis para a senha:** Selecione esta caixa de seleção para usar uma variável para a senha. Essa variável é definida em **Variáveis de modelo** em **Tipo de dados sensíveis**. Insira o nome da variável na caixa de Senha entre sinais de percentagem (%variablename%). Para mais informações, veja "Definir uma variável de modelo" na página 442.
- **Senha:** Digite a senha para fazer login no dispositivo. Confirme a senha na caixa **Confirmar senha**.
- **Parâmetros adicionais passados para a configuração:** Parâmetros a serem passados ao o arquivo de instalação quando ele for executado. Para Winnt32, o identificador de Provisionamento completa automaticamente os argumentos unattend (/unattend) e source (/s). Esses são gerados do caminho dado no caminho Winnt32 e do script selecionado.
- **Script de instalação:** o arquivo unattend usado na instalação do sistema operacional.
- **Forçar reinicialização:** Selecione esta caixa de seleção para exigir um reinicia depois que o SO foi instalado.

Linux

- **Local do initrd:** O local do arquivo inicial de RAMdisk. O padrão é /x86pc/undi/provlinux/initrd.img.
- **Local do Kernel:** O local do kernel do Linux.

- **Parâmetros adicionais passados na inicialização:** parâmetros a serem passados ao initrd quando for executado.
- **Script de instalação:** o arquivo unattend usado na instalação do sistema operacional.

Desinstalar serviço (somente a seção de Configuração do sistema)

Desinstalar um serviço no dispositivo alvo.

- **Nome do serviço:** o nome do serviço a ser desinstalado.

Descompactar arquivo (todas as seções)

descompacta o conteúdo de um pacote para um local predeterminado. Essa ação pode restaurar a estrutura original.

- **Caminho fonte e nome de arquivo:** o caminho e o nome do arquivo de pacote que será descompactado.
- **Caminho de destino:** o local em que o pacote será descompactado. Se houver um diretório/pasta existente, quaisquer nomes de arquivos duplicados serão sobrescritos.
- **Criar diretório de destino se ele ainda não existir:** Se o destino não existir, selecione esta caixa de seleção para criá-lo automaticamente.

Atualizar Registro (somente a seção de Configuração do sistema)

Esta ação adiciona ou remove chaves ou valores do registro ou importa um arquivo de registro (.reg). A edição incorreta do Registro pode danificar o sistema e até torná-lo inoperante. Antes de alterar o Registro, faça backup dos dados importantes do seu computador.

Selecione uma operação na lista **Operações de registro**.

- **Excluir chave:** remove a pasta e o caminho esperados da chave do Registro.
- **Excluir valor:** remove o valor esperado da chave.
- **Criar chave:** cria uma pasta no lado esquerdo do Editor do Registro.
- **Importar arquivo:** importa um arquivo do Registro.
- **Definir valor:** Criar um valor. O dado inserido é interpretado como um valor determinado pela lista **Tipo**.
- **Chave:** insira a chave a ser criada ou excluída.
- **Valor:** insira o valor a ser criado ou excluído.
- **Datum:** Digite os dados a serem salvos em um valor.
- **Tipo:** Selecione um tipo de dados. Ele pode ser um valor de string, string expandida, binário, DWord ou Multi-string.
- **Conteúdo do arquivo de importação:** Digite uma descrição do arquivo de registro a ser importado.
- **Importar dados do arquivo do Registro:** Digite o caminho completo do arquivo de registro ou clique em **Procurar** para localizá-lo, em seguida, clique em **Importar arquivo**.

Aguardar (todas as seções)

Pausa a execução de modelo por um tempo especificado ou até a criação de um arquivo solicitado.

- **Hora**: Pause a execução de modelo por um período de tempo.
- **Número de segundos a esperar:** Digite o número de segundos para pausar o modelo.

- **Arquivo:** Pause a execução de modelo até que um arquivo seja criado.
- **Esperar o arquivo existir:** Pausa a ação até que o caminho e o arquivo especificados surjam. É útil quando uma ação requer um aplicativo para instalar um arquivo. Quando o arquivo é criado, a próxima ação no modelo é executada.
- **Número máximo de segundos a esperar:** Insira o número de segundos para esperar para o arquivo ser criado. Se o tempo passa e o arquivo não é criado, o modelo continua com a próxima ação.

Propriedades de modelo

Use a tela **Propriedades** de modelo para mostrar os modelos atual ao momento em que o modelo foi criado.

Para ver as propriedades do modelo

1. Clique em **Ferramentas > Distribuição > Distribuição de SO**.
2. Em Provisionar modelos, clique em **Público** ou **Meus modelos** ou em um de seus subgrupos.
3. Clique com o botão direito em um modelo e clique em **Propriedades**. São mostradas as seguinte informações:

    - **Nome do modelo:** o nome do modelo.
    - **Descrição:** a descrição do modelo.
    - **Nome do proprietário:** O servidor núcleo e o nome de login da pessoa que tem direitos para executar o modelo. Se o modelo estiver numa pasta Públcia, esse nome é Usuário público.
    - **Ambiente de inicialização:** O ambiente de pré-inicialização no qual o modelo inicializa (Windows PE).
    - **SO alvo:** o sistema operacional alvo do modelo (por exemplo: Windows, Windows Vista, Windows 2008 Server, Linux, SuSE Pro 9.3 ou Red Hat 4 Workstation).

O modelos na pasta Meus modelos são visíveis a outros usuários mas só podem ser editados pelo criador ou pelos usuários com direitos administrativos.

LANDesk SmartVue

Bem-vindo ao LANDesk SmartVue

Use o LANDesk® SmartVue para exibir informações importantes sobre processos de TI que afetam a a produtividade do usuário, o desempenho do sistema e a segurança dos terminais. O SmartVue mostra a importância da TI em sua empresa e é ideal para Diretores de informação (CIOs), Chefes de departamento e Diretores de TI que precisam de informações em tempo hábil para tomada de decisões e conversas de negócios.

O SmartVue oferece dados para que você compartilhe os sucessos, desafios ou necessidades do deparamento de TI. Você também pode usá-lo para monitorar as metas, contratos de nível de serviço ou os principais indicadores de desempenho.

Com o SmartVue, você verá gráficos e diagramas em tempo real no seu iPhone ou iPad, gerados a partir de dados de gerenciamento de segurança de dados armazenados em seu servidor núcleo da LANDesk, como:

- Dispositivos gerenciados
- Sistemas operacionais
- Processos de patch
- Gerenciamento de energia
- Provisionamento
- Controle remoto
- Segurança
- Software
- Distribuição de software
- Atualizações do Windows

Outros recursos principais:

- Informações compartilhadas via exportação de PDFs
- Filtros de hora e local de todos os registros
- Integração com iBooks para impressão diretamente de seu iPhone or iPad
- Conectividade com outros produtos da LANDesk, como o Service Desk

Instalação do SmartVue

O instalador do SmartVue exige um servidor núcleo LANDesk Management Suite 9.5. Existem dois tipos de instalação do SmartVue:

- **Núcleo de pontoPonto central:** Um núcleo de ponto coleta dados do servidor núcleo onde está instalado e em outros núcleos que você especificar. Em seguida, o núcleo de ponto fornece os dados para o aplicativo SmartVue. Você só deve ter um núcleo de ponto em sua rede. A interface de usuário de configuração do SmartVue é somente no ponto central.
- **Núcleo remoto:** Um núcleo remoto ou núcleo de link lento envia dados do SmartVue para o núcleo de ponto na hora que você especificar. Considere usar isso em núcleos que se comunicam por um link de rede lento com o núcleo de ponto, ou a núcleos que possuem restrições de tempo de acesso.

Ao instalar o SmartVue em um núcleo de ponto, o programa de instalação instala os componentes, serviços de suporte da Web e a interface de configuração.

Ao instalar o SmartVue em um núcleo remoto, os dois únicos arquivos instalados são o LDGatherData.exe e o LANDesk.SmartVue.sahred.dll. Você pode executar manualmente o arquivo executável aqui:

- C:\Arquivos de progama (x86)\LANDesk\ManagementSuite\LDGatherData.exe

Este programa envia dados da consulta do SmartVue para o núcleo de ponto. Em núcleos remotos, você vai precisar agendar a execução deste arquivo executável manualmente, para quando quiser. Para isso, você pode utilizar o agendador de tarefas do Windows ou o agendador local do Management Suite.

Para instalar o SmartVue em um servidor núcleo de ponto

1. Se o console do LDMS estiver em execução no servidor núcleo onde você está instalando, saia dele.
2. No imagem de instalação do SmartVue, execute o arquivo setup.exe .
3. Na janela de **Boas vindas**, clique em **Avançar**.
4. Na tela **Contrato de licença**, clique em **Aceitar**.
5. Na janela de **Pré-requisitos**, clique em **Continuar**.
6. Na tela **O que você quer instalar?**, clique em **Servidor núcleo de ponto**. Se você estiver instalando o SmartVue em um servidor de núcleo remoto, clique nele e clique em **Continuar**.
7. Na página 'pronto para instalar', clique em **Instalar**.
8. Ao terminar a configuração, clique em **Concluir**.

Após instalar o SmartVue em um servidor núcleo de ponto, você precisa agendar a coleta de dados do SmartVue e configurar as fontes de dados adicionais (se tiver). Para obter mais informações, consulte "Agendamento da coleta de dados do SmartVue" na página 465 e"Configuração das fontes de dados do SmartVue" na página 466 .

Agendamento da coleta de dados do SmartVue

O aplicativo SmartVue não exibe os dados em tempo real. Cada componente no aplicativo SmartVue iOS é direcionado por uma série de consultas de banco de dados. Essas consultas precisam de ser executadas periodicamente e o aplicativo exibirá dados baseados nas últimas consultas. Para obter mais informações, consulte "Modificando componentes do SmartVue" na página 469.

Ao instalar o SmartVue pela primeira vez no núcleo de ponto, você pode querer iniciar um ciclo imediato de coleta de dados do SmartVue assim que tiver alguns dados para ver na aplicativo.

Para programar um ciclo imediato de coleta de dados do SmartVue

1. No console de gerenciamento, clique em **Configurar > Configuração do SmartVue**e clique na página **Agendador**.
2. Clique em **Iniciar agora** e em **OK** .
3. Monitore o andamento da tarefa com a ferramenta Tarefas agendadas. Clique em **Ferramentas > Distribuição > Tarefas agendadas** e em **Todas as tarefas > SmartVue** .

Após ter alguns dados do SmartVue no banco de dados, você pode agendar uma coleta periódica de dados. A maioria dos componentes coletam dados mensalmente, portanto, executar a coleta de dados uma vez por dia funciona bem.

Para agendar um ciclo periódico de coleta de dados do SmartVue

1. No console de gerenciamento, clique em **Configurar > Configuração do SmartVue**e clique na página **Agendador**.
2. Clique em **Repetir**.
3. Selecione um calendário: **Horário, Diário**ou **Semanal.**
4. Configure o intervalo escolhido.
5. Clique em **OK**.

Configuração das fontes de dados do SmartVue

Por padrão, o SmartVue recolhe dados do núcleo de ponto onde foi instalado. Você pode acrescentar outras fontes de dados, se desejar

Existem duas opções de fonte de dados padrão na caixa de diálogo de **configuração do Smartvue**, o **LANDesk Management Suite** e o **LANDesk Service Desk.** Se o banco de dados ao qual você está se conectando é um desses tipos, certifique-se de definir o tipo de fonte de dados para combinar.

Se você estiver se conectando a uma fonte de dados personalizada, você pode usar seu próprio nome. O nome da **Fonte de dados** sensível à letras maiúsculas e minúsculas que você inserir aqui também deverá ser inserido na configuração do arquivo .XML do componente ao qual se refere. O atributo que precisa corresponder é <DataDefinition datasource="">.

Para configurar fontes de dados

1. No console de gerenciamento, clique em **Configurar > Configuração do SmartVue**e clique na página **Banco de dados**.
2. Clique em **Adicionar** ou selecione uma fonte de dados existente e clique em **Editar**.
3. Insira as informações da fonte de dados e credenciais do banco de dados. Se o banco de dados é Oracle, selecione **Este é um banco de dados Oracle**. Clique em **Ajuda** para obter mais informações.
4. Clique em **OK**. Uma mensagem de erro será exibida se as informações que você forneceu não permitirem que o núcleo de ponto conecte-se com o banco de dados configurado.

Configuração dos locais do SmartVue

Se você gerenciar dispositivos em várias locai, você pode configurar o SmartVue para grupos de dispositivos por local. Use a página **Local** (**Configurar > Configuração do SmartVue** e clique na página **Localização**) para configurar como o SmartVue determina a localização do dispositivo. Você terá três opções:

- LDAP
- Nome do dispositivo
- Consultas públicas do LDMS

Você só pode escolher um único método de localização.

Configuração de locais do LDAP

Quando o analisador de inventário analisa um dispositivo gerenciado que pertence a um Active Directory, o analisador apresenta o caminho do local daquele dispositivo. Você pode informar ao SmartVue qual parte desse caminho contém o texto que informa o local que você deseja usar.

Na página **Local**do diálogo de **Configuração do SmartVue**, selecione LDAP . A página mostra um exemplo de caminho de localização informado pelo analisador de inventário. No campo de texto abaixo, o caminho do modelo relaciona elementos no caminho baseado nos delimitadores que você especificou (/ é o padrão). Selecione o elemento do caminho que contém o texto do local que você quer que o SmartVue.

Configuração de locais dos nomes do dispositivo

Se os dispositivos gerenciados têm um prefixo padronizado de localização nos seus nomes (por exemplo, prefixo de três letras de uma cidade), você pode inserir aqui. Você terá que inserir a posição e comprimento do caractere inicial. Selecione os caracteres na entrada do modelo e a caixa de diálogo preencherá os valores da sua seleção automaticamente. O primeiro caractere no nome do dispositivo está na posição 1, e não 0.

Você só pode configurar um único modelo de local de nome de dispositivo.

Configuração dos locais das consultas públicas do LDMS

Se você tem consultas que identificam os computadores por local, você pode usar a opção de local de consulta pública. Todos os resultados da consulta correspondem a um local. Você pode adicionar várias consultas. Após selecionar as consultas desejadas, clique no nome no **Nome do local** da consulta e personalize-a. O **Nome do local** é o nome exibido nos resultados do componente.

Usando o aplicativo SmartVue iOS

Antes de poder usar o aplicativo SmartVue iOS, você precisa:

1. Instale o SmartVue no servidor do núcleo que será seu núcleo de ponto. Para obter mais informações, consulte "Instalação do SmartVue" na página 464.
2. Agendar e executar o utilitário de coleta de dados do SmartVue (LDGatherData.exe) para que os dados do seu núcleo de ponto fique disponível para o aplicativo SmartVue iOS.
3. Permita que os usuários do aplicativo SmartVue façam o logon no núcleo de ponto a partir de aplicativos móveis (**Ferramentas > Administração > Gerenciamento de usuários**). Os administradores da LANDesk têm essa permissão por padrão.
4. (Opcional) Configure conexões adicionais do banco de dados com outros servidores de núcleo, servidores do LANDesk Service Desk ou fontes de dados personalizados.
5. Instale o aplicativo iOS em seu dispositivo móvel. Faça o download do aplicativo "LD-SmartVue" no iTunes: https://itunes.apple.com/us/app/ld-smartvue/id572070098.

Após atender os pré-requisitos acima, você pode fazer o logon em seu núcleo de ponto.

Para conectar-se a um núcleo de ponto do SmartVue a partir do aplicativo iOS

1. No seu dispositivo móvel, inicie o SmartVue.
2. Na caixa de diálogo de **Configurações**, insira o **Nome de usuário** e **Senha** da LANDesk.
3. O **Núcleo URL** será http://<nome do computador de seu núcleo de ponto ou endereço IP>. Por exemplo, http://myLANDeskcore.

Depois de conectar o aplicativo você pode procurar os dados que o utilitário de coleta de dados obteve. Consulte a tela de ajuda se você quiser saber como usar a aplicativo:

A aplicativo iOS se conecta ao núcleo de ponto para obter dados do componente quando você exibir uma categoria pela primeira vez e quando você mudar de categoria. Navegar em uma categoria não atualizará os dados do componente.

Arquitetura do SmartVue

Núcleos de pontos tem três serviços da Web. Os serviços da Web usa o serviço de token STS existente no servidor núcleo para autenticação/segurança.

- **SmartVueData:** Aceita dados postados por LDGatherData.exe.
- **SmartVue:** Fornece dados para o aplicativo móvel do SmartVue.
- **Dashboard1:** Gerencia a exibição do componente no aplicativo móvel do SmartVue.

A configuração cria essas novas tabelas no banco de dados do núcleo:

- SmartVueData:
- SmartVueLocationData
- SmartVueQueryLocations
- SmartVueComponentes
- SmartVueUserComponentes
- SmartVueConnections
- SmartVueSettings

O LDGatherData.exe envia os resultados ao serviço da Web do SmartVueData, que insere os dados nas tabelas do SmartVueData e do SmartVueLocationData.

Em conexões lentas, o LDGatherData.exe é instalado localmente. Você pode agendar a execução sempre que quiser. Ao terminar, o programa coleta os arquivos XML mais recentes do núcleo de ponto e envia os dados ao serviço da Web do SmartVueData do núcleo de ponto.

Modificando componentes do SmartVue

Cada categoria do componente SmartVue é definida em um arquivo XML que o instalador do SmartVue coloca no núcleo de ponto. Você pode modificar estes arquivos XML para adicionar, mudar ou remover componentes exibidos no aplicativo móvel SmartVue. Os arquivos XML são armazenados aqui no núcleo de ponto:

- C:\Arquivos de progama (x86)\LANDesk\ManagementSuite\SmartVueDef.

NOTA: Quando o programa LDGatherData.exe do SmartVue é executado, ele cria uma pasta .\SmartVue que também contém arquivos XML. Não edite esses arquivos. Se você modificar um arquivo XML .\SmartVueDef, o arquivo correspondente em .\SmartVue será substituído quando o arquivo LDGatherData.exe for executado.

Certifique-se de criar um backup de todos os arquivos XML que você pretende editar antes de realizar as alterações.

Esta é a estrutura básica do XML:

```
<?xml version="1.0" encoding="utf-8" ?>
<DataDefinition name="" id="" datasource="">
  <Definitions>
    <Definition name="" id="" controlType="" dataSet="">
      <Sql>
      </Sql>
      <TotalSQL>
      </TotalSQL>
      <LocationSQL>
      </LocationSQL>
      <Controls>
        <Control title="" columns="" />
      </Controls>
    </Definition>
  </Definitions>
</DataDefinition>
```

Cada componente contém uma definição de componente e três conjuntos de consultas.

- **<SQL>:** Coleta dados para o componente.
- **<Total SQL>:** Consulta os dados coletados do SQL e envia os dados para o componente.
- **<Location SQL>:** Combina os resultados da consulta ao Total SQL com as informações do local que foi configurado no núcleo de ponto. No núcleo de ponto, configure locais em **Configurar > Configuração do SmartVue > Local**. Você pode definir locais baseados em um diretório LDAP, uma string do prefixo de nome de dispositivo do computador, ou uma consulta pública ao LDMS.

As seções a seguir fornecem mais detalhes sobre os atributos do elemento XML.

<DataDefinition>

- **nome:** O nome da categoria. Este nome é usado na seção da condição ONDE do <TotalSQL> .
- **id:** O ID exclusivo desta definição. Este ID é usado na string de consulta do navegador. Não pode conter espaços ou caracteres como &.
- **fonte de dados:** O tipo de fonte de dados do banco de dados. É sensível à letras maiúsculas e minúsculas e deve corresponder exatamente a **Fonte de dados** que você especificou na caixa de diálogo **Adicionar banco de dados(Configurar > Configuração do SmartVue > Banco de dados**, clique em **Adicionar** ou **Editar**).

<Definition>

- **nome:** O título do componente. Este nome é usado na seção da condição ONDE do <TotalSQL> .
- **id:** O ID exclusivo deste componente. Não pode conter espaços.
- **controlType:** O tipo de componente a ser usado com esses dados. Deve ser um dos seguintes:
  - BarTemplate
  - BurnDownTemplate
  - ColumnTemplate
  - DonutTemplate
  - LineTemplate
  - PercentBallTemplate
  - PercentBarTemplate
  - PieTemplate
  - RadialTemplate
- **dataSet:** O formato dos dados é "linha" ou "coluna". Por exemplo, se o conjunto de dados retornado está no formato onde o dado 1 está na coluna 1, o 2 na coluna 2, e assim por diante, o conjunto de dados é "coluna". Se a instrução SQL retornar várias linhas, ela deve ser "linha".
- **seriesData:** Especificar "bymonth" (mensal) se isso for para dados de componente baseados em tempo. Você pode ver exemplos disso no arquivo Remotecontrol.xml. Isso funciona bem em modelos baseados em barras.

<SQL> ou <SQLOracle>

Contém as consultas SQL ou Oracle que obtém dados para o componente.

Se o SQL exigir funções específicas do Oracle, você pode incluir aquele SQL no <SQLOracle>. Se o SQL é genérico você não precisa fazer isso. Isso se aplica a todas as instruções específicas do Oracle.

<TotalSQL> ou <TotalSQLOracle>

Contém as consultas SQL ou Oracle que obtém dados para o componente.

A ordem e os nomes das colunas são importantes. O nome da coluna deve ser o primeiro. Se você quiser diferente de "Contagem de dados" ou "Contagem", você precisa nomear a primeira coluna como DataName (selecione a.columname DataName, …). A contagem deverá ser a segunda coluna na lista selecionada e ela deve ser chamada de DataCount. Se tiver dados de linha, deverá ser SUM. (selecione a.columnname DataName, SUM(a.DataCount) DataCount, …).

Se você deseja que seus dados sejam exibidos por data (no eixo y), o alias ReportDate deve ser a última coluna na cláusula SELECT (selecione a.columnname DataName, SUM(a.DataCount) DataCount, a.ReportDate A PARTIR DE…).

A condição a.CountType="" deve conter o <DataDefinition name=""> e o <Definition name=""> que você especificou no arquivo XML, sem espaços entre os nomes.

Por exemplo, se o nome <DataDefinition name="Power Management"> e <Definition name="Dispositivos sob Gerenciamento de energia">, a.CountType= poderia ser "Gerenciamento de energiaDispositivos sob Gerenciamento de energia".

Itens que que não são SQL nas consultas da seção TotalSQL

#SVTABLE# é um espaço reservado usado para determinar se as consultas estão procurando por dados em locais específicos ou não. Este espaço reservado é substituído dinamicamente.

Os espaços reservados #SVWHERE# e #SVTIME# são utilizados para determinar se a consulta deverá ser baseada na localização ou tempo, dependendo da seleção que usuário fizer no aplicativo. Existem dois tipos de componentes, baseado em tempo (muitas vezes representados por gráficos de barra) ou baseados na localização (muitas vezes representados por gráficos de pizza). Dados baseados em localização geralmente não têm relação com um período de tempo. Componentes baseados no tempo usam contagens de dados mensais.

<LocationSQL> ou <LocationSQLOracle>

Agrupa dados ao local.

Defina locais no núcleo de ponto clicando em **Configurar > Configuração do SmartVue > Local**. Você pode definir locais baseados em um diretório LDAP, uma string do prefixo de nome de dispositivo do computador, ou uma consulta pública ao LDMS. Você só pode escolher um.

<Controles>, <Título do controle>

Define os dados de linha ou coluna e os títulos que o componente deve exibir. Esta seção não é atualmente usada pelo SmartVue.

Ativando os componentes

Ao adicionar ou mudar arquivos XML na pasta C:\Program Files (x86) \LANDesk\ManagementSuite\SmartVueDef, as alterações não serão visíveis no aplicativo móvel do SmartVue até que o programa de coleta de dados seja executado:

- C:\Arquivos de progama (x86)\LANDesk\ManagementSuite\LDGatherData.exe

Se você agendou uma coleta de dados para o SmartVue, ele será executado conforme agendado. Se você quiser executá-lo imediatamente, faça o seguinte.

Para atualizar os dados do SmartVue

1. Clique em **Configurar > Configuração do SmartVue > Agendador**.
2. Clique em **Iniciar agora**.
3. Clique em **OK**.

O processo LDGatherData.exe vai levar alguns minutos para concluir.

Sobre a caixa de diálogo Configuração do SmartVue

A caixa de diálogo Configuração do SmartVue (**Configurar > Configuração do SmartVue**) só está disponível nos núcleos de ponto do SmartVue. Use esta caixa de diálogo para configurar as conexões com banco de dados do SmartVue, métodos de localização e horários de coleta de dados.

- "Sobre a página Banco de dados" na página 472
- "Sobre a página Localização" na página 472
- "Sobre a página Agendador" na página 472

Sobre a página Banco de dados

Use a página **Banco de dados** para adicionar fonte de dados do banco de dados onde SmartVue deve obter dados. Para obter mais informações, consulte "Configuração das fontes de dados do SmartVue" na página 466.

Sobre a caixa de diálogo Adicionar banco de dados

- **Fonte de dados:** Se você estiver se conectando com um banco de dados do Management Suite ou do Service Desk , selecione de acordo ou insira o nome da fonte de dados desejada.
- **Nome de exibição:** Um nome descritivo para sua fonte de dados. Este nome aparece na principal lista de banco de dados de configuração do SmartVue.
- **Servidor:** O nome do computador que hospeda o banco de dados para o qual você está criando uma conexão.
- **Banco de dados:** O nome do banco de dados no servidor que você especificou.
- **Nome de usuário** e **Senha** As credenciais do banco de dados que concedem acesso ao banco de dados.
- **Este é um banco de dados Oracle:** Selecione esta opção se o banco de dados for Oracle.

Ao clicar em **OK**, o SmartVue irá usar as informações fornecidas para se conectar ao banco de dados. Se a conexão, você verá uma mensagem de erro com mais informações.

Sobre a página Localização

Use a página de **Local** para configurar como o SmartVue determina localização do dispositivo. Você terá três opções:

- LDAP
- Nome do dispositivo
- Consultas públicas do LDMS

Para obter mais informações, consulte "Configuração dos locais do SmartVue" na página 466.

Sobre a página Agendador

A página do **Agendador** controla quando o utilitário de coleta de dados do SmartVue, o LDGatherData.exe, é executado. Este utilitário reúne dados do núcleo de ponto onde está instalado e todas as outras fontes de dados você configurou. Este utilitário não é executado automaticamente ou tem uma programação por padrão. Você agendar uma execução automática ou deve executá-lo manualmente.

A página **Agendador** tem as opções a seguir:

- **Deixar sem agendar:** Esta é a opção padrão. O LDGatherData.exe não está agendado para execução.
- **Iniciar agora:** O LDGatherData.exe é executado quando você clica em **OK** . Se você configurou o uma programação recorrente, ela será apagada. Se você quiser continuar a programação recorrente depois de usar a opção **Iniciar agora**, você vai ter que remarcar **Repetir** e reconfigurá-la**.**
- **Repetir:** Executa o LDGatherData.exe na programação recorrente especificada. Você pode escolher intervalos de **Hora**, **Dia**, ou **Semana**. Se você selecionar por hora, o programa é executado (TBD que hora?) cada hora. Se você selecionar **Diariamente** , você pode selecionar a hora que quiser. Se você selecionar **Semanalmente**, você pode selecionar o dia da semana e a hora que quiser.

Contas locais

Visão geral das contas locais

Contas locais é uma ferramenta administrativa usada para gerenciar os usuários e grupos nos computadores locais na sua rede. Através do console, é possível adicionar e excluir usuários e grupos, adicionar e remover usuários de grupos, definir e mudar senhas, editar configurações de usuário e grupo, e criar tarefas para reconfigurar senhas de vários dispositivos. Para o gerenciamento de contas locais funcionar, o LANDesk Agent padrão precisa ser instalado. Se um dispositivo for desligado e não estiver conectado à rede, não será possível usar as contas locais para gerenciá-lo.

NOTA: Ao usar contas locais, o núcleo interage com outros dispositivos quase em tempo real.

Gerenciar grupos de usuários locais

Adicione, exclua e edite grupos em um computador local usando o console.

Para adicionar um grupo

1. No console, da **Tela de rede**, clique em **Dispositivos > Todos os dispositivos**.
2. Clique com o botão direito no dispositivo que quer gerenciar e selecione **Gerenciar usuários e grupos locais**.
3. Na caixa de diálogo **Usuários e grupos locais**, clique com o botão direito em **Grupos** e, em seguida, em **Adicionar**.
4. Na caixa de diálogo **Novo grupo**, digite um nome de grupo e uma descrição.
5. (Opcional) Adicione usuário ao grupo clicando em **Adicionar**.
6. Clique em **Salvar**.

Para excluir um grupo

1. No console, da **Tela de rede**, clique em **Dispositivos > Todos os dispositivos**.
2. Clique com o botão direito no dispositivo que quer gerenciar e selecione **Gerenciar usuários e grupos locais**.
3. Na caixa de diálogo **Usuários e grupos locais**, clique em **Grupos**.
4. Clique com o botão direito no grupo que deseja excluir e, em seguida, clique em **Excluir**.
5. Clique em **Sim** para confirmar o procedimento.

Para editar um grupo

1. No console, da **Tela de rede**, clique em **Dispositivos > Todos os dispositivos**.
2. Clique com o botão direito no dispositivo que quer gerenciar e selecione **Gerenciar usuários e grupos locais**.
3. Na caixa de diálogo **Usuários e grupos locais**, clique em **Grupos**.
4. Clique com o botão direito no grupo que deseja editar e, em seguida, clique em **Editar**.
5. Faça as alterações nas propriedades do grupo e clique em **OK**.

Gerenciar usuários locais

Adicione, exclua e edite usuários em um computador local usando o console.

Para adicionar um usuário

1. No console, da **Tela de rede**, clique em **Dispositivos > Todos os dispositivos**.
2. Clique com o botão direito no dispositivo que quer gerenciar e selecione **Gerenciar usuários e grupos locais**.
3. Na caixa de diálogo **Usuários e grupos locais**, clique com o botão direito em **Usuários** e, em seguida, em **Adicionar**.
4. Na caixa de diálogo **Novo usuário**, digite um nome de usuário, um nome completo e uma descrição.
5. Digite uma senha, confirme a senha e especifique as configurações da senha.
6. Clique em **Salvar**.

Para excluir um usuário

1. No console, da **Tela de rede**, clique em **Dispositivos > Todos os dispositivos**.
2. Clique com o botão direito no dispositivo que quer gerenciar e selecione **Gerenciar usuários e grupos locais**.
3. Na caixa de diálogo **Usuários e grupos locais**, clique em **Usuários**.
4. Clique com o botão direito no usuário que deseja excluir e, em seguida, clique em **Excluir**.
5. Clique em **Sim** para confirmar o procedimento.

Para editar um usuário

1. No console, da **Tela de rede**, clique em **Dispositivos > Todos os dispositivos**.
2. Clique com o botão direito no dispositivo que quer gerenciar e selecione **Gerenciar usuários e grupos locais**.
3. Na caixa de diálogo **Usuários e grupos locais**, clique em **Usuários**.
4. Clique com o botão direito no usuário que deseja editar e, em seguida, clique em **Editar**.
5. Faça as alterações nas propriedades do usuário e clique em **OK**.

Designar usuários à grupos

A partir do console, há dois métodos de adicionar e remover usuários de grupos em um cliente local. O primeiro método permite adicionar ou remover usuários de um grupo uma vez. O segundo permite adicionar ou remover o usuário selecionado de um ou mais grupos.

Para adicionar usuários a um grupo

1. No console, da **Tela de rede**, clique em **Dispositivos > Todos os dispositivos**.
2. Clique com o botão direito no dispositivo que quer gerenciar e selecione **Gerenciar usuários e grupos locais**.
3. Na caixa de diálogo **Usuários e grupos locais**, clique em **Grupos**.
4. Clique com o botão direito no grupo que deseja editar e, em seguida, clique em **Editar**.
5. No diálogo **Editar grupo**, clique em **Adicionar**.

6. Selecione os usuários que deseja adicionar ao grupo e clique em **Adicionar>>**.
7. Clique em **OK**.
8. Clique em **OK** na caixa de diálogo **Editar grupo**.

Para adicionar um usuário a um ou mais grupos

1. No console, da **Tela de rede**, clique em **Dispositivos > Todos os dispositivos**.
2. Clique com o botão direito no dispositivo que quer gerenciar e selecione **Gerenciar usuários e grupos locais**.
3. Na caixa de diálogo **Usuários e grupos locais**, clique em **Usuários**.
4. Clique com o botão direito no usuário que deseja adicionar a um ou mais grupos e, em seguida, clique em **Editar**.
5. Na caixa de diálogo **Editar usuários**, clique na guia **Membro de**.
6. Clique em **Adicionar**.
7. Selecione os grupos aos quais deseja que o usuário pertença e clique em **Adicionar>>**.
8. Clique em **OK**.
9. Clique em **OK** na caixa de diálogo **Editar usuário**.

Para remover usuários de um grupo

1. No console, da **Tela de rede**, clique em **Dispositivos > Todos os dispositivos**.
2. Clique com o botão direito no dispositivo que quer gerenciar e selecione **Gerenciar usuários e grupos locais**.
3. Na caixa de diálogo **Usuários e grupos locais**, clique em **Grupos**.
4. Clique com o botão direito no grupo de onde deseja remover usuários e, em seguida, clique em **Editar**.
5. Selecione os usuários que deseja remover e clique em **Remover>>**.
6. Clique em **OK**.

Para remover um usuário de um ou mais grupos

1. No console, da **Tela de rede**, clique em **Dispositivos > Todos os dispositivos**.
2. Clique com o botão direito no dispositivo que quer gerenciar e selecione **Gerenciar usuários e grupos locais**.
3. Na caixa de diálogo **Usuários e grupos locais**, clique em **Usuários**.
4. Clique com o botão direito no usuário que deseja remover de um ou mais grupos e, em seguida, clique em **Editar**.
5. Na caixa de diálogo **Editar usuários**, clique na guia **Membro de**.
6. Selecione os grupos dos quais deseja que o usuário seja removido e clique em **Remover>>**.
7. Clique em **OK**.

Mudar a senha de uma conta local

Mude senhas de usuários em computadores locais usando o console.

Para mudar uma senha de usuário.

1. No console, da **Tela de rede**, clique em **Dispositivos > Todos os dispositivos**.
2. Clique com o botão direito no dispositivo que quer gerenciar e selecione **Gerenciar usuários e grupos locais**.
3. Na caixa de diálogo **Usuários e grupos locais**, clique em **Usuários**.
4. Clique com o botão direito no usuário do qual deseja mudar a senha e clique em **Definir senha**.
5. Digite a nova senha, confirme-a e clique em **OK**.
6. Clique em **OK** para verificar se a senha foi mudada corretamente.

Redefinir uma senha de conta local

Crie uma tarefa agendada para reconfigurar a senha de um nome de usuário específico. Quando a tarefa tiver sido agendada, é aberta a ferramenta **Tarefas agendadas** onde você pode especificar os dispositivos alvo e o horário de início. Por exemplo, em uma conta local, você pode criar uma tarefa para reconfigurar a senha do nome de usuário **Administrador**. A seguir, você atribui os dispositivos alvo e agenda o horário de ocorrência da tarefa. Após a tarefa ter sido executada, todos os administradores que quiserem autenticar-se nos dispositivos alvo terão que usar a nova senha.

Para reconfigurar a senha

1. No console, da **Tela de rede**, clique em **Dispositivos > Todos os dispositivos**.
2. Clique com o botão direito no dispositivo que quer gerenciar e selecione **Gerenciar usuários e grupos locais**.
3. Na caixa de diálogo **Usuários e grupos locais**, clique em **Usuários**.
4. Clique no ícone **Agendar**.
5. Na caixa de diálogo **Agendar tarefa**, insira o nome do usuário para quem deseja reconfigurar a senha. Selecione um nome de usuário já existente na lista ou digite outro nome.
6. Digite a nova senha, confirme-a e clique em **Agendar**.
7. Na ferramenta **Tarefas agendadas**, clique com o botão direito na tarefa agendada e clique em **Propriedades**.
8. No diálogo **Tarefas agendadas - propriedades**, atribua dispositivos alvo e digite as informações de agendamento.
9. Clique em **Salvar**.

Usar a ferramenta contas locais no servidor núcleo

O servidor núcleo é um nó na rede com contas locais, portanto, você pode usar a ferramenta contas locais para realizar tarefas administrativas no servidor assim como administrar o próprio console. Você pode adicionar usuários LANDesk ao console criando usuários locais e adicionando-os ao grupo LANDesk Management Suite Windows, LANDesk Script Writers ou LANDesk Administrators. Isso permite a execução de tarefas administrativas do console, sem ter que usar o sistema de gerenciamento nativo das contas como, por exemplo, o Gerenciamento de computador no Windows.

Se preferir, você pode ainda usar o sistema de gerenciamento nativo de contas locais para gerenciar as contas locais. Acesse os dispositivos diretamente, controle computadores remotamente do console ou use uma ferramenta de terceiros para acessar os dispositivos e realizar tarefas administrativas.

Para mais informações sobre o uso do console para o gerenciamento de contas locais, consulte "Gerenciamento de usuários" na página 38.

Ajuda do gerenciamento de contas locais

Sobre a caixa de diálogo Novo usuário

Use essa caixa de diálogo para criar um novo usuário. Para obter mais informações, consulte "Gerenciar usuários locais" na página 475.

- **Nome de usuário:** especifica o nome de usuário do novo usuário.
- **Nome completo:** especifica o nome completo do usuário.
- **Descrição:** fornece uma descrição do usuário.
- **Senha:** especifica uma senha para o usuário autenticar no console.
- **Confirmar senha:** confirma a senha.
- **O usuário deve mudar a senha na próxima vez que acessar:** obriga o usuário a mudar a senha no acesso inicial ao console.
- **O usuário não pode mudar a senha:** desautoriza os usuários a mudarem a senha.
- **A senha nunca vence:** faz com que a senha nunca vença e assim o usuário não precisa mudá-la.
- **A conta está desativada:** desativa a conta.

Sobre a caixa de diálogo Editar

Use esta caixa de diálogo para editar as propriedades do usuário. A caixa de diálogo consiste em três guias de configuração, **Geral**, **Membro de**, e **Perfil**.

Para obter mais informações, consulte "Gerenciar usuários locais" na página 475.

Guia geral

Use esta página de configuração para especificar o nome do usuário, o nome completo e a descrição do usuário. Você também pode mudar algumas das propriedades da conta.

- **Nome de usuário:** especifica o nome do usuário (se disponível).
- **Nome completo:** especifica o nome completo do usuário.
- **Descrição:** especifica a descrição do usuário
- **O usuário deve mudar a senha na próxima vez que acessar:** Especifica se o usuário precisa mudar a senha ao acessar o console.
- **O usuário não pode mudar a senha:** especifica se o usuário pode mudar a senha.
- **A senha nunca vence:** especifica se a senha tem validade
- **A conta está desativada:** especifica se a conta está desativada.
- **A conta está bloqueada:** esta opção fica disponível quando a conta está bloqueada. As conta são geralmente bloqueadas quando o usuário tenta, sem sucesso, acessar a sua conta mais de três vezes em uma sessão. Esta opção desbloqueia a conta para que o usuário possa autenticar-se no console.

Guia Membro de:

use essa página de configuração para atribuir o usuário a grupos.

- **Grupos selecionados:** relaciona os grupos dos quais o usuário é membro.
- **Adicionar:** abre a caixa de diálogo **Selecionar grupos**, a qual o habilita a adicionar os grupos aos quais quer que o usuário pertença.
- **Remover:** remove o usuário dos grupos selecionados e remove os grupos da lista.

Perfil

Use esta página de configuração para especificar as informações de conta do usuário.

- **Caminho de perfil do usuário:** especifica o caminho da rede para a conta e o perfil do usuário.
- **Script de logon:** especifica os scripts de logon.
- **Caminho local:** especifica um caminho local como diretório principal.
- **Conectar:** especifica um diretório de rede como diretório principal. Selecione uma unidade e insira o caminho de rede.

Sobre a caixa de diálogo Propriedades do grupo

Use essa caixa de diálogo para configurar o grupo. Para obter mais informações, consulte "Gerenciar grupos de usuários locais" na página 474.

- **Nome do grupo:** especifica o nome do grupo.
- **Descrição:** fornece uma descrição do grupo.
- **Membros:** relaciona os usuários que pertencem ao grupo.
- **Adicionar:** inicia a caixa de diálogo **Selecionar usuários**, a qual o habilita a adicionar usuários ao grupo.
- **Remover:** remove os usuários selecionados do grupo.

Gerenciamento de dispositivos Macintosh

Visão geral do Gerenciamento de dispositivos móveis da Macintosh

O LANDesk Management Suite fornece gerenciamento de sistemas para computadores e dispositivos Apple Macintosh. Isso ajuda a automatizar tarefas de gerenciamento de sistemas na empresa inteira. No console de gerenciamento da LANDesk, você pode:

- Colete e analise dados detalhados de inventários de hardware e software de cada dispositivo
- Use os dados para selecionar alvos para distribuição de software e estabelecer diretivas para gerenciamento de configuração automatizado.
- Gerencie licenças de software para economizar custos e monitorar a conformidade com os contratos de licença.
- Dispositivos de controle remoto para resolver problemas ou realizar manutenção de rotina.
- Proteja seus dispositivos de uma variedade de riscos de segurança e de estar exposto
- Mantenha o controle do seu inventário e produza relatórios informativos.

Este capítulo descreve como usar o LANDesk Management Suite para gerenciar computadores Macintosh. Relaciona informações específicas sobre tarefas relacionadas a Macintosh, ferramentas, recursos e funcionalidade. Para informações mais amplas sobre o uso de ferramentas e recursos de gerenciamento de rede, consulte a seção de ajuda de cada ferramenta.

Versões de SO compatíveis

O LANDesk Management Suite para funcionalidade no Macintosh é compatível com as seguintes versões de SO do Mac X:

- 10.5 (Leopard)
- 10.6 (Snow Leopard)
- 10.7 (Lion)
- 10.8 (Mountain Lion)

Suporte a herdados

Mac OS X: 10.2 (Jaguar), 10.3 (Panther), 10.4 (Tiger)

O agente LANDesk Management Suite versão 9.5 para Macintosh não suporta Jaguar, Panther ou Tiger. Entretanto você pode ainda gerenciar dispositivos executando esses sistemas operacionais se eles tiver o agente LANDesk Management Suite versão 8.8 para Macintosh neles instalado.

Para obter mais informações sobre como fazer o download deste agente legacy, consulte o seguinte documento da comunidade LANDesk: http://community.landesk.com/support/docs/DOC-21797.

NOTA: Devido a diferenças de diretiva entre a versão 8.8 e a versão 9.0, o gerenciamento baseado em diretiva não funcionará com clientes Jaguar e Panther usando o agente versão 8.8.

Mac OS 9

É possível usar inventário e controle remoto com os dispositivos Mac OS 9. Este SO está para ser descontinuado e o suporte é limitado.

Configuração de agente de dispositivos Macintosh

O LANDesk Management Suite utiliza configurações de agente para ganhar o controle de dispositivos e gerenciá-los. As configuração de agente Macintosh são enviados para dispositivos Macintosh não gerenciados usando o mesmo processo usado para enviar agentes para dispositivos Windows.

Carregamento da configuração de agente padrão para dispositivos Macintosh

O pacote Configuração padrão Mac contém o agente requerido para controle de dispositivos Macintosh. Para ganhar o controle dos dispositivos Macintosh, é necessário:

1. Obter o pacote necessário (agentes).
2. Distribuir os agentes para os dispositivos.

Após a instalação dos agentes padrão, os dispositivos Macintosh tornam-se dispositivos gerenciados. Você pode criar configurações personalizadas para ter maior controle desses dispositivos. Os agentes personalizados são facilmente implementados assim que os dispositivos são gerenciados.

NOTA: Todos os dispositivos devem oferecer suporte a TCP/IP.

Obtenção do pacote (agentes) para dispositivos Macintosh

Você pode obter o pacote padrão **Default_Mac_Configuration.mpkg.zip** da pasta compartilhada LDLogon/Mac no seu servidor núcleo. A pasta LDLogon/Mac é criada automaticamente durante a instalação do Management Suite. Por ser um compartilhamento da Web, a pasta LDLogon está disponível na Internet no site em http://<CoreServerName>/LDLogon/Mac.

Distribuição de agentes para dispositivos Macintosh que usam Secure Shell (SSH)

Para colocar agentes nos dispositivos Macintosh que têm Secure Shell (SSH) ativado, é necessário especificar as credenciais de login SSH para os dispositivos Mac não gerenciados selecionando **Configurar > Serviços > Agendador > Alterar login** no console do Windows. Você pode usar a mesma distribuição de agente por envio que usaria para os dispositivos Windows.

Distribuição e instalação de agentes para dispositivos Macintosh que não usam Secure Shell (SSH)

Para colocar agentes em dispositivos Macintosh que não têm Secure Shell (SSH) ativados, você precisará escolher um método de distribuição alternativo como:

- Acesse o agente usando um navegador da Web no LDLogon/Mac e envie pacotes de configurações por e-mail aos usuário.
- Gravar o pacote de configuração em um CD ou em outra mídia removível e levá-lo para cada dispositivo Macintosh e instalá-lo manualmente.

Após distribuir os agentes para os dispositivos alvo, é necessário instalá-los nos dispositivos. Uma análise completa de hardware e software é feita no final de todas as instalações. Isso sincroniza os dispositivos com o servidor núcleo. É necessário que os agentes LANDesk estejam instalados nos dispositivos Macintosh e as informações de inventário sejam enviadas ao servidor núcleo para poder gerenciá-los. Após instalar os agentes básicos, as distribuições subseqüentes de agentes e as atualizações são manipuladas com facilidade através dos agentes existentes.

Para instalar o agente LANDesk em um dispositivos Macintosh

1. Na máquina do cliente, localize o **Default Mac Configuration.pkg.zip** ou acesse o pacote no compartilhamento na Web (http://<CoreServerName>/LDLogon/Mac).
2. Descompacte o arquivo ou copie os arquivos dispositivo alvo.
3. Clique duas vezes em **LDMSClient.mpkg**.
4. Reinicie a máquina após a instalação do pacote.

Distribuição de configurações de agente para dispositivos Macintosh

Use a ferramenta Configuração de agente para criar e atualizar (substituir) as configurações personalizadas para os dispositivos Macintosh. Você pode criar diferentes configurações para as suas necessidades específicas como, por exemplo, mudar as configurações do analisador de inventário, permissões de controle remoto ou os protocolos de rede usados pelo agente.

Para enviar as configurações para os dispositivos, é necessário criar ou atualizar uma configuração de agente e agendar uma tarefa.

Criar ou atualizar a configuração de agente

Definir configurações específicas para seus dispositivos. Não use parêntesis nos nomes de configuração do agente no Macintosh. Isso causará falha na distribuição da tarefa.

Para criar uma configuração de agente para dispositivos Macintosh

1. Clique em **Ferramentas > Configuração > Configuração de agentes**.
2. Selecione um grupo de configurações (Minhas configurações ou configurações públicas). Na barra de ferramentas, clique em **Nova configuração de agente** > **Nova configuração do agente Mac**.
3. Preencha as opções na caixa de diálogo **Configuração de agente**. Para obter mais informações, consulte "Uso da caixa de diálogo Configuração de agente (para Macintosh)" na página 483 ou clique em **Ajuda** na caixa de diálogo.
4. Clique em **Salvar**.

Para atualizar uma configuração de agente

1. Clique em **Ferramentas > Configuração > Configuração de agentes**.
2. Clique com o botão direito do mouse na configuração de agente a ser atualizada e selecione **Propriedades**.
3. Faça as atualizações à configuração do agente.
4. Clique em **Salvar**.

Agendar a configuração do agente

Instale por envio configurações de agente a dispositivos com agente LANDesk padrão instalado. Use a ferramenta **Tarefas agendadas** para distribuir sua configuração de agente nova ou atualizada.

Para agendar uma configuração de agente para dispositivos Macintosh

1. Clique em **Ferramentas > Configuração > Configuração de agentes**.
2. Clique com o botão direito do mouse na configuração do agente a ser agendada e selecione **Agendar distribuição de agente**.
3. Arraste dispositivos, grupos ou consultas da tela de rede até a tarefa para os dispositivo alvo da tarefa.
4. Selecione a tarefa, clique em **Propriedade**s na barra de ferramentas e agente uma hora para iniciá-la.

Execução manual da configuração de agente para dispositivos Macintosh

Você pode executar configurações de agente manualmente para dispositivos Macintosh assim que eles tiverem sido criados ou atualizados. Quando uma configuração de agente o seguinte arquivo é criado na pasta LDLogon/Mac no seu servidor núcleo:

- **<agent configuration name>.mpkg.zip**

A pasta LDLogon/Mac é um compartilhamento da Web e deve ser acessível de qualquer navegador. Siga as instruções para a instalação do agente (consulte "Para instalar o agente LANDesk em um dispositivos Macintosh" na página 482), mas insira o seu nome de arquivo de configuração de agente no lugar do nome padrão.

Remoção de agentes Macintosh

Para desinstalar agentes Macintosh, execute **uninstallmacagent.sh** de \\<core>\ldmain.

Uso da caixa de diálogo Configuração de agente (para Macintosh)

Esta seção descreve a caixa de diálogo da configuração de agente para dispositivos Macintosh. Essa caixa de diálogo contém as seguintes páginas:

- Iniciar
- Application policy management (APM)
- Inventário
- Controle remoto
- Agente LANDesk padrão
- Análise de patch e conformidade
- Ocupante

Sobre a página Inicial

- **Nome de configuração**: Digite um nome para a configuração de agente.
- **Configuração padrão:** Marque esta caixa de seleção para tonar esta a configuração de agente padrão do Macintosh
- **Não execute o Menu de status do cliente:** Marque esta caixa de seleção se não quiser que usuários vejam o menu da barra de status que permite a execução de instalações e análises.

Sobre a página de Gerenciamento de diretiva de aplicativo

Use esta página para configurar parâmetos para o agente de distribuição baseada em diretiva.

- **Número da porta TCP:** Especifica a porta que o agente de distribuição baseado em diretiva usará para comunicar-se com o servidor núcleo. A porta padrão é 12176. Será preciso certificar-se de que essa porta está aberta em todos as firewalls entre os dispositivos e o servidor núcleo. Se essa porta for modificada, será necessário modificá-la também no servidor núcleo. É possível mudar a porta que o servidor QIP usa, para isso, edite a seguinte chave de registro: HKLM\Software\Intel\LANDesk\LDWM\QIPSrvr
- **Executar quando o endereço IP mudar:** Se selecionado, é iniciada uma análise quando o endereço IP muda.
- **Mudar configurações:** Mudar configurações e configurar uma agenda personalizada baseada em hora, dia da semana ou mês e se o usuário está conectado. O agendamento padrão é executar uma análise a todo dia com um demora aleatória de até uma hora.

Sobre a página Inventário

Use essa página para configurar o analisador de inventário.

- **Envie análise para o servidor núcleo do LDMS:** Envia as informações da os resultados da análise para o banco de dados do servidor núcleo.
- **Salvar análise no diretório:** O diretório onde os dados da análise foram salvos. Se selecionar a opção servidor núcleo e esta opção, as informações de análise irão para ambos os locais.
- **Escolha de componentes de análise:** Selecione os componentes que deseja analisar. Se nenhum componente for selecionado, a velocidade de análise pode aumentar ligeiramente.
- **Forçar análise de software:** Força o dispositivo a fazer uma análise de software com cada análise de inventário, independentemente do servidor núcleo indicar que uma está vencida.
- **Executar quando o endereço IP mudar:** O disparo do endereço IP envia apenas uma mini análise para o servidor núcleo, que torna o inventário muito mais rápido nas mudanças de endereço IP.
- **Mudar configurações:** Muda os parâmetros e configura uma agenda local personalizada em hora, dia da semana ou mês, se um usuário está conectado. O agendamento padrão deve ser executado todos os dias com um adiamento aleatório de até uma hora.

Sobre a página de Controle remoto

Use essa página para configurar o agente de controle remoto.

- **Modelo local:** Esta é a segurança mais básica que utiliza as configurações de controle remoto que estiverem especificadas no dispositivo. Este modelo não requer nenhuma outra autenticação ou participação em grupo.
- **Segurança integrada:** Esta é a opção mais segura. A segurança integrada segue este fluxo de comunicação:
    1. O usuário do controle remoto se conecta ao agente do controle remoto do dispositivo gerenciado, mas o agente responde que é necessária uma autenticação de segurança integrada.
    2. O usuário pede direitos de controle remoto do servidor núcleo.
    3. O servidor núcleo calcula os direitos de controle remoto baseado no escopo do usuário, direitos de administração com base em funções e direitos do Active Directory. O servidor núcleo, então, cria um documento assinado e seguro e o devolve ao usuário.
    4. O usuário envia esse documento ao agente de controle remoto no dispositivo gerenciado, o qual verifica o documento assinado. Se tudo estiver correto, o agente permite o início do controle remoto.

- **Permissão necessária:** Pede ao usuário permissão para ser controlado remotamente sempre que alguém iniciar uma sessão remota. Se o usuário não estiver ao computador ou negar a permissão, a sessão remota não iniciará.
- **Abrir aplicativos e arquivos:** Permite ao usuário remoto abrir arquivos neste dispositivo.
- **Copiar itens:** Permite ao usuário remoto copiar arquivos de e para esse dispositivo.
- **Excluir e renomear itens:** Permite que um usuário remoto exclua ou renomeie arquivos que residem neste dispositivo.
- **Bloquear teclado e mouse:** Permite que um usuário remoto bloqueie o seu teclado e mouse durante uma sessão de controle remoto. Essa opção impede que você interfira com ações remotas.
- **Tela em branco:** Permite que um usuário remoto faça a sua tela ficar vazia durante uma sessão de controle remoto. Essa opção será útil se o seu dispositivo contiver documentos sigilosos que um administrador talvez precise abrir remotamente sem deixar que outros usuários os leiam, caso se aproximem do monitor do dispositivo.
- **Reiniciar e desligar:** Permite que um usuário remoto reinicie ou desligue o seu dispositivo.
- **Controlar e observar:** Permite que um usuário remoto controle e observe suas ações neste dispositivo. O administrador não pode fazer nada mais além de observar as ações.
- **Alerta ao observar:** Quando uma sessão de controle remoto está ativa, exibe uma dica visual na barra de menus.

Sobre a página do agente LANDesk padrão

Use essa página para configurar o escopo da segurança e gerenciamento do agente. Para obter mais informações sobre a segurança de agente, consulte "Segurança de agente e certificados confiáveis" na página 108. Para obter mais informações, consulte "Gerenciamento de usuários" na página 38.

- **Certificados confiáveis:** Lista os certificados no servidor núcleo. O cliente deve ter um certificado que corresponde ao certificado no servidor núcleo para a comunicação de agente se autorizada. Esses certificados são usados para autenticar a comunicação do agente. Você pode digitar um nome de domínio ou endereço IP para o cliente usar ao se comunicar com o servidor núcleo. O agente de controle remoto para Macintosh não usa certificados.
- **Caminho:** Define o atributo de inventário de local do computador do dispositivo. Os escopos são usados pela administração com base em função do para controlar o acesso do usuário aos dispositivos e podem ser baseados neste caminho de diretório personalizado. Esse caminho é opcional.

Sobre a página de análise de Patch e conformidade

Use esta página para configurar o agendamento para análises de patch e conformidade.

- **Mudar configurações:** Muda os parâmetros e configura uma agenda local personalizada em hora, dia da semana ou mês, se um usuário está conectado. O agendamento padrão deve ser executado todos os dias com um adiamento aleatório de até uma hora.
- **Use o servidor de atualizações alternativo:** Especifique um servidor núcleo diferente para atualizações de Patch e conformidade se o servidor núcleo principal não estiver disponível.
- **Configurações de análise e reparo:** Selecione as configurações que você deseja usar nas análises de patch e conformidade.
- **Configurar:** Visualizar todas as configurações de análise e reparo. Edite ou crie novas configurações e selecione as configurações ou crie novas configurações para usar nas análises de patch e conformidade.

Sobre a página do ocupante

Use esta página se você tem o complemento Gerenciamento de ocupantes do Management Suite. Você pode designar uma configuração de agente para um ocupante em sua empresa.

- **Atribua um ocupante para esta configuração:** Marque esta caixa de seleção se a configuração de agente da Macintosh for usada somente por um ocupante em sua empresa.
- **Escolha um ocupante:** Selecione um ocupante na lista de ocupantes disponíveis definidos no console de gerenciamento da LANDesk.

Conectar ao servidor núcleo através do Utilitário de serviços na nuvem da LANDesk

Existem duas opções de configuração de dispositivos Macintosh gerenciados para conectar ao núcleo através do Utilitário de serviços na nuvem da LANDesk (conhecido como LANDesk Management Gateway):

- Faça o envio da configuração para dispositivos portáteis enquanto eles estão conectados à rede local. Este é um modo fácil de configurar dispositivos móveis para poderem conectar-se através do Utilitário de serviços na nuvem da LANDesk após serem desconectados da rede local. Este tipo de configuração habilita a funcionalidade do LANDesk Management Suite através do utilitário, sem a necessidade de configurar manualmente dispositivos gerenciados individuais.
- Configure manualmente cada dispositivo gerenciado no Utilitário de serviços na nuvem da LANDesk. Este tipo de configuração habilita a funcionalidade do LANDesk Management Suite através da utilitário. A configuração manual só pode ser feita por um usuário com direitos de Administrador no dispositivo cliente.

Envie a configuração para dispositivos portáteis enquanto eles estão conectados à rede local.

- Após configurar o núcleo para conexão através do Utilitário de serviços na nuvem da LANDesk, recompile os agentes para dispositivos Macintosh e envie-os para os dispositivos. Para obter mais informações, consulte Configurar o Utilitário de serviços na nuvem da LANDesk (Management Gateway).

Para configurar manualmente um dispositivo gerenciado:

1. Na pasta **Utilitários** no dispositivo gerenciado, inicie o Utilitário de serviços na nuvem da LANDesk.
2. Especifique o **Nome do domínio** do utilitário.
3. Escolha o melhor método de conexão para o núcleo LANDesk.
4. Solicite um certificado digitando um nome de usuário e senha de console LANDesk e clicando em **Solicitar**.
5. Clique em **Testar** para testar a conexão do dispositivo gerenciado do Utilitário de serviços na nuvem da LANDesk.
6. Se o resultado do teste apresentar falha, verifique as informações digitadas, corrija os erros que houver e clique em **Testar** para assegurar-se de que a conexão está funcionando.
7. Se o dispositivo gerenciado acessar a Internet através de um proxy, especifique as configurações de proxy necessárias.

Executar a Análise de inventário em dispositivos Macintosh

O utilitário de análise de inventário é usado para adicionar dispositivos Macintosh ao banco de dados núcleo e para coletar dados de hardware e software de dispositivos. Ao configurar um dispositivo o analisador de inventário é um dos componentes do agente LANDesk instalados no dispositivo. A análise de inventário é automaticamente executada quando o dispositivo é inicialmente configurado. Um dispositivo é considerado gerenciado quando envia uma análise de inventário ao banco de dados núcleo.

O executável da análise para o Mac OS X denomina-se **ldiscan** (UNIX é sensível a maiúsculas e minúsculas). Os arquivos de análise de inventário são salvos localmente no cliente e são compatíveis com o núcleo. Você pode enviar o arquivo via e-mail ao administrador núcleo e depois arrastá-lo e soltá-lo no diretório ldiscan. É necessário mudar a extensão do arquivo para .scn.

Os dispositivos Macintosh podem ser configurados para fazer a análise na inicialização, no login, na ativação de repouso e na mudança de rede. É possível também usar a configuração agente para agendar a análise de inventário para ocorrer a intervalos regulares.

A análise de inventário Macintosh criptografa as análises. A análise de inventário também usa análises delta para que, após a análise inicial de inventário completa, análises subseqüentes enviem somente os dados modificados ao servidor núcleo. Isso reduz o consumo de largura de banda na rede.

A análise de inventário Macintosh procura (na pasta "Dados personalizados", sob a pasta instalação de agente) os arquivos XML que contêm informações adicionais as quais você deseja que a análise de inventário passe ao servidor núcleo. Essas informações adicionais são mostradas na árvore de inventário sob o nó Dados personalizados.

Com o analisador de inventário, você pode ver o resumo de dados de inventário ou dados completos. Você pode imprimir e exportar os dados de inventário. Também é possível usá-lo para definir consultas, agrupar dispositivos e gerar relatórios especializados.

Análise de software

Uma análise de software compila um inventário de software nos dispositivos gerenciados. Essas análises levam mais tempo para serem executadas que as análises de hardware. As análises de software podem levar alguns minutos para terminar, dependendo do número de arquivos no dispositivo gerenciado. O intervalo de análise de software pode ser configurado na guia **Configurar > Serviços > Inventário**.

Todos os aplicativos instalados na pasta Aplicativos são colocados no nó **Software > Suites de aplicativo** na árvore de inventário.

Parâmetros de linha de comando do analisador

Você pode adicionar parâmetros de linha de comando às propriedades do atalho (ldiscan) da análise de inventário para controlar como ela funciona. A opção é sensível a maiúsculas/minúsculas.

NOTA: A menos que a opção **--ignore** seja configurada, as opções de linha de comando não cancelam as configurações nas preferências de configuração de análise. Por exemplo, a especificação de **-F** para análise completa de software não realiza a análise de software se ela estiver desativada nas preferências.

Opção	Nome	Descrição
-c	--núcleo <path>	Especifica o núcleo ao qual a análise é enviada. Exemplo: -c spencercore2.landesk.com
-D	--Delta	Força uma análise delta
-e	--tudo	Forces uma análise completa de hardware e software
-F	--força	Força uma análise de software mesmo quando nenhuma das opções de análise tenham sido selecionadas na configuração do agente. Exemplo: [MACHINES_MACX] REMEXEC0=/Library/Application\ Support/LANDesk/bin/ldiscan –F
-h	--ajuda	Mostra uma lista de opções de linha de comando
-i	--ignorar	Ignora as configurações de preferência de usuário e servidor
-l	--LdAppl <caminho>	Especifica o caminho alternativo para LdAppl.ini
-L	--Limite	Limita o download de LdAppl3.ini
-o	--saída <caminho>	Especifica onde o arquivo de análise deve ser enviado. Exemplo: -o /Users/spencer
-P	--Print	Mostra as configurações de análise sem analisar
-R	--redefinir	Reconfigura o banco de dados da análise
-s	--sincronizar	Executa uma análise de sincronização (e implica -R)
-T	--enviar <arquivo>	Envio o <arquivo> para o núcleo
-t	--mini	Executa uma mini análise
-v	--versão <n>	Dá as informações formatadas de versão (1,2 ou 3)
-V	--Verbostiy <n>	Define o nível de verbosidade (depuração)

Editar o arquivo LdAppl3.Template

O arquivo LdAppl3.Template contém os parâmetros de inventário da análise. Esse arquivo de modelo trabalha com o arquivo LdAppl3 para identificar o inventário de software de um dispositivo.

Você pode editar a seção [LANDesk Inventory] do arquivo modelo para configurar os parâmetros que determinam como o analisador identifica o inventário de software. Por padrão, o LdAppl3.Template está localizado no diretório do servidor núcleo:

- \Arquivos de programas\LANDesk\ManagementSuite\LDLogon

Use esta tabela como um como guia para ajudar a editar a seção [LANDesk Inventory] em um editor de texto.

Opção	Descrição
MacMode	Determina como o analisador verifica o software Macintosh nos dispositivos. O padrão é Todos. As configurações são as seguintes: • **Listado:** Registra os arquivos listados em LdAppl3. • **Não listado:** Registra os nomes e as datas de todos os arquivos com as extensões listadas na linha MacScanExtensions, mas que não foram definidas no LdAppl3. Esse modo ajuda a descobrir o software não autorizado na rede. • **Todos:** Descobre arquivos com extensões contidas na linha MacScanExtensions.

Você deve selecionar **Tornar disponíveis aos clientes** para permitir o download de MacModes. Os MacScanExtensions são ativados por padrão. Isso pode criar arquivos de análise muito grandes (11 MB+), por isso pode ser necessário mudar esse padrão.

NOTA: Por padrão, os diretórios /Library ou /System não são analisados na análise MacScanExtensions. Isso reduz o tamanho do arquivo de análise. Os diretórios podem ser colocados na seção include da pasta Mac.

Análise de dados personalizados

Para inteirar-se das informações sobre análise para datos personalizados, consulte "Verificação de dados personalizados em dispositivos da Macintosh" na página 173.

Controle remoto de dispositivos Macintosh

Você pode controlar remotamente um dispositivo Macintosh no console da mesma forma que o faria em um dispositivo Windows. Antes de poder realizar qualquer tarefa de controle remoto, é necessário conectar ao dispositivo alvo. Somente um visualizador pode se comunicar com um dispositivo por vez, embora você possa abrir várias janelas e controlar dispositivos diferentes ao mesmo tempo.

Ao conectar-se a um dispositivo, você pode ver as mensagens e o status da conexão no painel **Mensagens da conexão** (**Ver > Mensagens de conexão**). A segurança integrada do Management Suite verifica se o usuário iniciando a sessão de controle remoto tem os direitos apropriados e se o computador é parte do escopo do usuário. Os dados são ofuscados ao passarem pela rede.

NOTA: Como padrão, a segurança integrada é ativada.

Para obter mais informações sobre o uso do controle remoto no Management Suite, veja "Controle remoto" na página 247.

Conectar a um dispositivo Macintosh

É possível conectar-se a um dispositivo Macintosh e usar o controle remoto no mesmo--você também pode usar o bate-papo, transferência de arquivos ou execução remota.

Para conectar-se a um dispositivo

1. Na **Tela de rede**, clique com o botão direito no dispositivo que desejar controlar remotamente, e selecione **Controle remoto**, **Bate-papo**, **Transferência de arquivo** ou **Executar remotamente**.
2. Quando a janela do visualizador for exibida e conectar ao dispositivo remoto, você poderá usar qualquer ferramenta de controle remoto disponível no menu **Ferramentas**, como bate-papo, transferência de arquivos, reinicialização, inventário ou controle remoto.
3. Para encerrar uma sessão de controle remoto, clique em **Arquivo > Interromper conexão**.

NOTA: Compartilhamento de área de transferência e recursos de desenho não são suportados nos dispositivos Macintosh.

Emulação do teclado do Macintosh

Os teclados Macintosh têm teclas que não são encontradas nos teclados de PCs. Ao usar o controle remoto em um dispositivo Macintosh, as seguintes teclas são usadas no teclado do PC para simular o teclado Macintosh:

- A tecla Alt mapeiam para a tecla Command.
- As teclas Windows mapeiam para a tecla Option.

É necessário ter a passagem de tecla do sistema habilitada na janela da tela do controle remoto para as teclas Alt passarem os mapeamentos Macintosh.

Controle remoto da linha de comando

É possível controlar remotamente um computador Mac da linha de comando em um computador que tiver o contêiner de controle remoto. Use o seguinte comando:

```
irccntr.exe /a[client name] /s[core name]
```

Tempo limite de inatividade:

O tempo limite de inatividade especifica um período (o padrão é 10 minutos) após o que, se o cliente não receber movimentos de mouse ou de tecla, a sessão é encerrada. A exemplo do recurso de proteção de tela, ele impede que outras pessoas usem o computador remoto quando não estiver sendo usado.

Distribua pacotes de softwares para dispositivos Macintosh

A distribuição de software permite distribuir pacotes de software e de arquivos a dispositivos Macintosh na rede executando Mac OS X.

Você pode distribuir pacotes executáveis de um único arquivo para dispositivo Mac OS X. Cada pacote distribuído consiste em apenas um arquivo e o agente tentará instalar o arquivo assim que o dispositivo o receber. Qualquer arquivo pode ser descarregado. Os pacotes de instalação (.pkg) também podem conter diretórios, mas devem ser compactados. Se o arquivo do download tiver um sufixo .dmg, .pkg, .mpkg, .sit, .sitx, .zip, .tar, .gz, .sea, .app, .sh, .hqx ou para pacotes Automator/fluxo de trabalho, o Management Suite descompactará o arquivo antes de retornar.

NOTA: Certifique-se que a opção "verificar novas versões" do Stuffit Expander está desativada; caso

contrário, uma caixa de diálogo provavelmente interromperá a execução da distribuição do software.

A distribuição de softwares também fornece a habilidade de distribuir scripts de shell como tarefas. Isso habilita você a ter ainda mais controle do ambiente operacional Mac e realizar fazer praticamente qualquer tarefa de configuração ou de reunir informações em um dispositivo Mac OS X.

Você pode agendar distribuições do OS Mac X na janela Tarefas agendadas e arrastar os dispositivo com SO Mac X até a janela de Tarefas agendadas como alvos de distribuição.

NOTA: Você deve instalar o agente Mac OS X da LANDesk nos dispositivos alvo antes de distribuir os arquivos para eles.

Um pacote de distribuição consiste em arquivos a enviar e detalhes de distribuição que descrevem os componentes e o comportamento do pacote. É necessário criar o pacote antes deste poder ser distribuído e executado. As seguintes instruções explicam como realizar uma distribuição de software. A fim de ser executado corretamente, o pacote de distribuição de software deve existir em um servidor de rede ou em um Servidor da Web e os dispositivos alvo devem ter um agente de distribuição de software instalado.

Distribua um pacote de software para dispositivos Macintosh

Há três etapas principais necessárias para distribuir um pacote para dispositivos:

1. Crie um script de pacote de distribuição para o software que desejar distribuir
2. Crie um método de entrega
3. Agendar uma tarefa de distribuição de software

Para criar um script de pacote de distribuição

1. Crie o pacote a ser distribuído.
2. Clique em **Ferramentas > Distribuição > Pacotes de distribuição**.
3. Em **Meus pacotes**, **Pacotes públicos** ou**Todos os pacotes**, clique em **Novo** na barra de ferramentas e selecione **Novo pacote do Macintosh**.
4. Na caixa de diálogo **Propriedades Macintosh**, insira as informações do pacote e configure as opções. Para obter mais informações sobre cada página, clique em **Ajuda**.
5. Clique em **Salvar** quando terminar. Seu pacote é exibido no item da árvore do tipo de pacote selecionado.

Para criar um novo método de entrega

1. Clique em **Ferramentas > Distribuição > Métodos de entrega**.
2. Expanda um grupo de métodos de entrega e clique com o botão direito do mouse no método de entrega que deseja usar e clique em **Novo método de entrega.**
3. Na caixa de diálogo **Método de entrega**, insira as informações de distribuição e altere as opções que desejar. Para obter mais informações sobre cada página, clique em **Ajuda**.
4. Clique em **Salvar** quando terminar. O seu script é exibido no item de árvore do método de distribuição selecionado.

NOTA: Se um pacote requer a reinicialização, o dispositivo alvo será reiniciado sem importar a seleção da opção na página de **Reinicialização** da caixa de diálogo**Métodos de entrega.** A opção **Nunca reinicializar** não é suportada na distribuição de pacotes da Macintosh, porque o dispositivo alvo pode tornar-se instável ou não reiniciar se um pacote não executar a reinicialização conforme esperado.

Para agendar uma tarefa de distribuição de software

1. Clique em **Ferramentas > Distribuição > Tarefas agendadas**.
2. Clique no botão **Criar tarefa de distribuição de software** na barra de ferramentas.
3. Na página **Visão geral**, insira o nome e o agendamento da tarefa. Reveja outras opções e clique em **Mudar** para alterar qualquer um deles.
4. Na página **Pacote de distribuição**, selecione o pacote de distribuição que criou.
5. Na página **Método de entrega**, selecione o método de entrega que desejar usar.
6. A página **Dispositivos alvo** não tem dispositivos listados. Dispositivos são alvos de distribuição depois de arrastá-los da tela de rede para a tarefa na ferramenta Tarefas agendadas.
7. A página **Mensagem personalizada** não se aplica a distribuição de pacotes da Macintosh.
8. A página **Agendar tarefa** é definida como **Deixar sem agendar**, a menos que você tenha dispositivos alvo.
9. Clique em **Salvar** quando terminar. O pacote está relacionado na ferramenta **Tarefas agendadas**.
10. Para distribuir o pacote, arraste dispositivos Macintosh da tela de rede na tarefa. Você pode arrastar dispositivos, grupos de dispositivos ou consultas para a tarefa.

A distribuição começa imediatamente. Veja o andamento da tarefa na janela Tarefas agendadas.

Comandos de distribuição de software Macintosh

Os comandos de distribuição de software do Macintosh são comandos de download, ao contrário do comando de shell. Os comandos de download começam com "http://" ou "ftp://". Se o comando não for um comando de download, por definição será um comando de shell. O seguinte é um exemplo de um comando de download:

```
REMEXEC0=http://...
```

Um comando de download não executará nenhum arquivo automaticamente. Depois de fazer download do arquivo para os dispositivos, você pode continuar com um comando de shell para executar o arquivo. O download dos arquivos são descarregados em /Library/Application Support/LANDesk/sdcache/, que você precisa conhecer para os comandos de shell.

NOTA: Se você estiver hospedando arquivos em um servidor Windows 2003, é necessário criar tipos MIME para as extensões de arquivo Macintosh, como .sit, caso contrário, o servidor 2003 não permitirá seu acesso aos arquivos. O tipo de MIME não precisa ser válido, só precisa existir.

Configurar diretivas para dispositivos Macintosh

Você pode também criar diretivas de dispositivo Macintosh. A criação de diretivas para um dispositivo Macintosh é semelhante à criação de uma diretiva para um dispositivo Windows. Os dispositivos Macintosh também têm os mesmos tipos de diretivas necessárias, recomendadas e opcionais. Os pacotes de aplicativos Macintosh devem ser de um formato de arquivo único. O gerenciamento baseado em diretivas verificará se há atualizações em um intervalo de quatro horas. Para diretivas opcionais ou recomendadas, o usuário cliente precisa iniciar o painel de preferências LANDesk e clicar em **Verificar agora** para a distribuição baseada em diretivas. Ao direcionar diretivas, os dispositivos Macintosh não suportam o gerenciamento de diretivas de aplicativos por nome de usuário, apenas por nome de dispositivo.

O gerenciamento baseado em diretivas faz o seguinte com os pacotes de diretivas de aplicativos do Macintosh:

1. Descarrega os arquivos para /Library/Applications/LANDesk/sdcache (assim como os downloads de distribuição de software).
2. Se o download estiver compactado, o gerenciamento baseado em diretivas o descompactará no local.
3. Se o download for uma imagem de disco, o gerenciamento baseado em diretivas irá montá-lo, procurar o primeiro arquivo do Apple Package Installer no volume montado, executá-lo silenciosamente e, em seguida, desmontá-lo.
4. Se o download for um arquivo do Apple Package Installer, o gerenciamento baseado em diretivas irá executá-lo silenciosamente.

Além disso, o gerenciamento baseado em diretivas oferece suporte a arquivos dmg com EULAs.

NOTA: Alguns tipos de pacote não funcionam bem com a distribuição de software. (O Installer Vise e os instaladores do Installer Maker não funcionam com o gerenciamento baseado em diretivas. Eles quase sempre exigem interação do usuário, podendo ser cancelados.)

Para adicionar uma diretiva de cliente Macintosh:

1. Clique em **Ferramentas > Distribuição > Métodos de entrega**.
2. Configure um método de entrega por envio suportado por diretiva ou por diretiva para o pacote que você desejar distribuir.
3. Clique em **Ferramentas > Distribuição > Tarefas agendadas**.
4. Clique no botão **Criar tarefa de distribuição de software** na barra de ferramentas.
5. Configure a tarefa. Clique em **Ajuda** em cada página para obter mais informações.

Para atualizar as diretivas do cliente local:

1. No aplicativo do agente LANDesk no dispositivo Macintosh, clique no ícone **Entrega**.
2. Clique em **Verificar agora** para o gerenciamento de diretivas de aplicativos.

Para visualizar as diretivas instaladas

- No painel Preferências do Management Suite do dispositivo Macintosh, clique na guia **APM**.

Mostre a interface de usuário ao cliente

Pode-se mostrar ou esconder a IU ao cliente durante a distribuição de um pacote de software. Se o administrador LANDesk estiver enviando um pacote que requer que o usuário selecione um contrato de licença, o pacote precisa ser instalado usando um método controlado pelo usuário. Isso é necessário porque o pacote não instalará o contrato de licença se este não for aceito pelo usuário final. Você pode mostrar a IU através do método de entrega baseada em envio ou diretiva.

Para mostrar a IU ao cliente durante a distribuição de software

1. Crie um novo método de entrega de distribuição de software ou selecione um método já existente para editá-lo.
2. Selecione **Feedback e horário** na árvore.
3. Selecione **Mostrar o andamento ao usuário** na lista **IU do progresso do pacote**.
4. Selecione Exibir interface completa do pacote.
5. Clique em **Salvar**.

Executa tarefas personalizadas com scripts gerenciados

O LANDesk Management Suite usa scripts para executar as tarefas personalizadas em dispositivos. Você pode criar scripts a partir da janela **Gerenciar scripts** (**Ferramentas > Distribuição > Gerenciar scripts**). Os scripts Macintosh usam comandos shell para executar arquivos. Os comandos de shell são executados como raiz. Os scripts são gravados como arquivos de texto e você poderá editá-los manualmente se precisar. O seguinte é um exemplo de um comando:

```
REMEXEC0=/Library/Application\ Support/LANDesk/bin/ldscan
```

O usuário pode usar o comando do shell "open" (abrir) para iniciar arquivos e aplicativos ou "installer" para instalar arquivos .PKG. O arquivo de download pode ser também um script de shell escrito em Perl, Ruby, Python e assim por diante.

Quando os arquivos são descarregados, eles são salvos em /Library/Application Support/LANDesk/sdcache/ e você precisa saber disso para executar alguns dos comandos de shell.

Você pode agendar scripts gerenciados do Mac OS X na janela Tarefas agendadas e arrastar os dispositivo Mac OS X até a janela de Tarefas agendadas como alvos de scripts.

Executar tarefas agendadas em dispositivos Macintosh

A ferramenta Tarefas agendadas ativa ou inicia muitas das tarefas que você define ou configura no aplicativo. Essas tarefas podem executar imediatamente, agendadas para outra hora ou configuradas para executar regularmente.

Para ver mais informações, consulte "Agendamento de tarefas" na página 227.

NOTA: Antes que você possa agendar tarefas para um dispositivo, o agente LANDesk padrão deverá estar instalado no dispositivo e o dispositivo deverá estar no banco de dados do inventário.

Os procedimentos a seguir requerem o uso da ferramenta Tarefas agendadas:

- Distribuição de configuração de agente
- Distribuição de software

- Scripts gerenciados
- Distribuição de sistema operacional
- Security and Patch Manager

Elaboração de relatório e monitoramento de licença de software

Os dispositivos Macintosh executando o Mac OS X suportam o Monitoramento de licenças de software. Com cada análise de inventário, o agente de monitoramento de software Macintosh envia para o servidor núcleo, as informações sobre os aplicativos que os dispositivos executam. A ferramenta de monitoramento de licenças de softwares mostra os aplicativos Macintosh juntamente com os aplicativos Windows.

Analise os arquivos baseado em suas extensões. O arquivo LdAppl3.ini contém a lista de extensões para análise. Por padrão, os arquivos tipo .dmg e .pkg são analisados. Você pode inserir extensões adicionais no arquivo LdAppl3.INI, localizado, por padrão, nas pastas **/Library /Applications /System /User**. O local do arquivo também pode ser modificado. Você também pode usar o arquivo LdAppl3.ini para analisar arquivos de multimídia.

O aplicativo de agente LANDesk pode ser usado para mostrar aplicativos que forma abertos e a frequência com que eles são usados.

Gerar relatórios para dispositivos Macintosh

A ferramenta de relatórios permite gerar uma grande variedade de relatórios especializados, que fornecem informações críticas sobre os dispositivos Macintosh gerenciados na sua rede. A ferramenta de relatórios opera da mesma forma para todos os sistemas operacionais. Para obter mais informações, consulte "Relatórios" na página 197.

Patch e conformidade para dispositivos Macintosh

Patch e conformidade é uma solução de segurança integrada que ajuda a proteger seus dispositivos Macintosh de uma variedade de riscos prevalentes de segurança e exposições. A ferramenta permite gerenciar o conteúdo de segurança e patches, analisar dispositivos, usar patches e corrigir dispositivos.

Configurar dispositivos Macintosh para análise de segurança e correção

É incluída a funcionalidade de segurança como parte do agente LANDesk padrão para dispositivos Macintosh. Ela permite a você analisar os dispositivos Macintosh para vulnerabilidades e executar correção distribuindo patches ou atualizações de software.

Como iniciar o analisador para dispositivos Macintosh

O analisador pode ser iniciado do console ou manualmente no computador cliente.

Para executar uma análise de conformidade do LANDesk Management Console

1. Clique em **Ferramentas > Segurança e conformidade > Patch e conformidade**.
2. Clique no botão **Criar uma tarefa** na barra de ferramentas e selecione **Análise de conformidade**.
3. Digite um nome para a tarefa e selecione **Criar uma tarefa agendada** ou **Criar uma diretiva**, dependendo de como você quer executar a análise.

4. Na ferramenta **Tarefas agendadas**, selecione a tarefa e clique no botão **Propriedades** na barra de ferramentas.
5. Especifique as opções de análise. Na página **Script personalizado** você especificará os detalhes da análise de conformidade.

Para obter mais detalhes sobre como criar uma tarefa de análise de conformidade, veja "Criar tarefas de análise de segurança e conformidade" na página 591

NOTA: Ao definir configurações de uma análise de conformidade, alguma funcionalidade não está disponível para dispositivos gerenciados da Macintosh. Aponte para itens em cada página da caixa de diálogo; uma mensagem indica quando um item não está disponível para análises no Macintosh.

Para iniciar a análise de segurança em um cliente Macintosh

1. Abra **Preferências do sistema** do Mac OS X no dispositivo alvo e selecione o painel **Cliente da LANDesk**.
2. Na guia **Visão geral**, clique na seção **Verificar agora** na seção Gerenciador segurança e patch.

Bloquear aplicativos para dispositivos Macintosh

Você pode usar a Ferramenta de Patch e conformidade Management Suite para bloquear aplicativos nos dispositivos Macintosh. Esta funcionalidade funciona da mesma forma que nos dispositivos Windows com a exceção de que não há conteúdo bloqueado pré-definido disponível para dispositivos Macintosh.

Você só pode bloquear arquivos .app em dispositivos Macintosh gerenciados. Para bloquear aplicativos específicos, você deve criar uma definição personalizada para cada aplicativo bloqueado. Quando criar a definição personalizada, cretifique-se de selecionar a opção **Aplicar ao Mac**.

Distribuição de sistema operacional (OSD) para dispositivos Macintosh

Você pode usar a distribuição de SO (OSD) com o agente da LANDesk para Macintosh usando NetBoot/NetInstall como parte do Servidor Mac OS X.

Para obter informações detalhadas, consulte os tópicos a seguir no documento da Comunidade da LANDesk: http://community.landesk.com/support/docs/DOC-5149

Acessar um dispositivo Mac através na tela do controle remoto

Use a tela do controle remoto para acessar um dispositivo remotamente. Você somente pode controlar remotamente dispositivos Windows e Mac que possuam o agente LANDesk instalado. Durante uma seção de controle remoto você terá os mesmos direitos e privilégios do usuário conectado no dispositivo remoto. Você pode realizar remotamente a maioria das tarefas que o usuário no dispositivo faz.

Quando você está controlando um dispositivo remoto, a tela desse dispositivo aparece na janela. Como a janela da tela não é tão grande como a tela de dispositivo remoto, será necessário usar as barras de rolagem para cima e para baixo e lateralmente, ou usar o recurso **Escala** para redimensionar a tela de representação remota, fazendo-a caber na janela da tela. A alteração na escala reduz a qualidade da imagem e se a tela for muito reduzida, será muito difícil ler o texto.

Você também pode aumentar a área de exibição desabilitando itens no menu **Sessão**, tais como os painéis de bate-papo e log ou a barra de ferramentas. Use a opção **Tela inteira** do menu **Visualizar** para remover completamente os controles da janela do visualizador. Se a resolução da tela remota ultrapassar a sua, a escala será ajustada para se adequar ao tamanho do seu monitor.

Se desejar tornar mais rápida a taxa de visualização ou alterar as configurações da janela, use a opção **Controle remoto LANDesk** no menu **Preferências** para exibir a caixa de diálogos **Opções**.

Para obter mais informações, leia as seguintes seções:

- Conexão a dispositivos
- Bate-papo com dispositivos remotos
- Envio de seqüências de teclas especiais
- Uso do controle remoto sem visualizar a tela remota
- Personalização do controle remoto

Conexão a dispositivos

Antes de poder realizar qualquer tarefa de controle remoto, é necessário conectar ao dispositivo alvo. Somente um visualizador pode se comunicar com um dispositivo por vez, embora você possa abrir várias janelas e controlar dispositivos diferentes ao mesmo tempo. Ao conectar-se a um dispositivo, você pode ver as mensagens e o status da conexão no painel de log, se ele estiver visível. Se não estiver, você pode exibi-lo clicando em **Sessão > Exibir log**.

Se desejar iniciar uma nova sessão, clique em **Arquivo > Novo**. Para parar uma sessão, clique em **Arquivo > Fechar**. Se a opção de menu **Sessão** estiver esmaecida, você não está conectado a um dispositivo.

Bate-papo com dispositivos remotos

Você pode usar a tela do controle remoto para bater papo remotamente com um usuário em um dispositivo remoto. Esse recurso é útil quando você precisa dar instruções a um usuário remoto cuja conexão dial-up está usando a única linha telefônica disponível. Os usuários podem responder usando a janela de bate-papo que aparece na tela deles. Você só pode usar o bate-papo em dispositivos que possuam o agente LANDesk for Mac instalado. Esse recurso funciona mesmo se você não estiver vendo a tela remota do dispositivo.

Você pode salvar as mensagens de uma sessão de bate-papo O texto que aparece na área cinza da sessão de bate-papo será salva em um arquivo de texto.

Para bater papo com um usuário em um dispositivo remoto

1. Assim que estiver conectado em um dispositivo remoto, clique em **Sessão > Exibir bate-papo**.
2. Uma janela de bate-papo aparece no lado direito da tela. A sessão superior mostra as mensagens enviadas e recebidas. A seção inferior é onde você pode digitar sua mensagem. Pressione 'Enter' para enviar a mensagem digitada.

Sua mensagem aparecerá na tela do dispositivo remoto. Um usuário pode responder digitando uma mensagem e clicando em **Enviar**. O usuário também pode clicar em **Fechar** para sair de uma sessão de bate-papo.

Para salvar mensagens de uma sessão de bate-papo

1. Na área de bate-papo da tela de controle remoto, clique em **Salvar mensagens**.
2. Na caixa de diálogo **Salvar como**, digite um nome de arquivo e clique em **Salvar**.

Envio de sequências de teclas da Macintosh

Os teclados Macintosh têm teclas que não são encontradas nos teclados de PCs. Ao usar o controle remoto em um dispositivo Macintosh, as seguintes teclas são usadas no teclado do PC para simular o teclado Macintosh:

- A tecla Alt mapeiam para a tecla Command.
- As teclas Windows mapeiam para a tecla Option.

É necessário ter a passagem de tecla do sistema habilitada na janela da tela do controle remoto para as teclas Alt passarem os mapeamentos Macintosh.

Uso do controle remoto sem visualizar a tela remota

Se não desejar ver a tela do dispositivo remoto mas desejar apenas bater papo com um usuário nele, você pode parar a observação.

Para parar de observar um dispositivo remoto mas ainda manter a conexão remota a ele

1. Enquanto conectado a um dispositivo remoto, clique em **Sessão > Não observar**. Você ainda pode usar o recurso de bate-papo com o dispositivo.
2. Clique em **Sessão > Observar** para restaurar a tela remota.

Personalização do controle remoto

Você pode personalizar as seguintes opções de controle remoto:

- Alteração das configurações de controle remoto
- Otimização do desempenho do controle remoto
- Personalização da barra de ferramentas

Alteração das configurações de controle remoto

Use a guia **Mudar configurações** da caixa de diálogo **Opções** (**Controle remotoLANDesk**> Preferências) para ajustar as configurações do controle remoto.

- **Bloquear o teclado e o mouse remotos:** Bloqueia o teclado e o mouse do dispositivo de modo que somente o usuário que estiver executando a janela do visualizador possa controlar o dispositivo remoto. Observe que as combinações de teclas especiais no Windows, como por exemplo, "Ctrl+Alt+Del" ou "Windows Key+L" não estão bloqueadas.
- **Ocultar a tela do computador remoto:** Oculta a tela do dispositivo remoto de modo que somente o usuário que estiver executando o visualizador possa ver a tela da interface do usuário no dispositivo remoto.
- **Gravar entradas de log em Remote.log:** Se desejar salvar um log das ações de controle remoto em um arquivo de log, marque esta opção. É possível selecionar três níveis de log, onde o nível 1 é o menos detalhado e o nível 3 é o mais detalhado. Nível 1 é o nível padrão.

Otimização do desempenho do controle remoto

Use a guia **Otimizar o desempenho** do diálogo **Opções(Controle remoto LANDesk > Preferências**) para otimizar o desempenho do controle remoto.

A mudança da configuração de otimização ajusta dinamicamente a redução de cor, a visibilidade do papel de parede e os efeitos de aparência das janelas remotas (aquelas que você pode ajustar no Windows em **Propriedades de tela | Aparência | Efeitos**) como efeitos de transição para menus e dicas de ferramentas.

O controle remoto sempre usa um algoritmo de compressão altamente eficiente para dados de controle remoto. Entretanto, mesmo com compressão ele requer muitos dados para enviar informações de profundidade de cor forte. Você pode reduzir substancialmente a quantidade de dados de controle remoto necessária reduzindo a profundidade de cor mostrada na tela do controle remoto. Quando a tela reduz a profundidade de cor, a tela tem que mapear a paleta completa de cor da desktop remota para um paleta de cor reduzida na tela. Como resultado, você pode notar as cores na janela remota que não refletem de forma precisa a desktop romota. Se isso for um problema, selecione uma configuração de compressão de qualidade mais alta.

Outra forma pela qual você pode otimizar o desempenho é **Suprimir o papel de parede remoto**. Quando você faz isso, o controle remoto não tem que enviar atualizações de papel de parede, pois partes da desktop remota estão descobertas. O papel de parede com freqüência inclui imagens de largura de banda intensiva, como fotos. Essas imagens não são compactadas muito bem e levam tempo para ser transferidas em conexões lentas.

Personalização da barra de ferramentas de controle remoto

Você pode personalizar qualquer botão que aparece na barra de ferramentas de controle remoto.

Para personalizar os botões da barra de ferramentas

1. Clique em **Sessão > Personalizar barra de ferramentas**.
2. Arraste os botões desejados da paleta para a tela da janela.
3. Arraste os botões que você não quer, da tela da janela para a paleta.
4. Para restaurar o layout padrão dos botões, arraste o conjunto padrão na parte inferior da paleta para a tela.

Você pode alterar o tamanho do botão clicando em **Usar tamanho menor**. Também é possível usar a opção **Exibir** para mostrar somente ícones, somente texto ou ambos.

Introdução ao LANDesk Security Suite

Bem-vindo ao LANDesk Security Suite

O LANDesk Security Suite fornece as ferramentas necessárias para gerenciar e proteger dispositivos e dados críticos na sua rede empresarial usando um único console.

O Security Suite é compatível com ambientes de rede heterogêneos que incluam cliente Windows, Macintosh e Linux.

O Security Suite é baseado na funcionalidade primária do LANDesk Management Suite que permite configurar e gerenciar dispositivos de rede e aperfeiçoa e concentra-se nessa funcionalidade adicionando ferramentas específicas relacionadas à segurança como, Patch e conformidade, Antivirus, Endpoint Security, HIPS, LANDesk Firewall, Device Control, 802.1X NAC (Network Access Control), Agent Watcher e outros; oferecendo uma solução abrangente e segmentada de segurança.

Solução abrangente e segmentada de segurança

O Security Suite é uma solução de gerenciamento de segurança completo que permite *monitorar de forma pró-ativa, avaliar, corrigir, verificar, defender e fortalecer a sua infra-estrutura e recursos de rede*.

A ferramenta fundamental Patch e conformidade o capacita a analisar e corrigir tipos predominantes de riscos de segurança que continuamente ameaçam o funcionamento e o desempenho dos seus dispositivos gerenciados e incluem: vulnerabilidades de sistema operacional e de aplicativos conhecidas, spyware, vírus, erros de configuração, aplicativos não autorizados ou proibidos e outras ameaças potenciais de segurança.

O LANDesk Antivirus permite fazer download das últimas atualizações de arquivo de definição de vírus. Configura também análises de vírus para verificar os dispositivos gerenciados e fornecer aos usuários finais opções para cuidar de arquivos infectados e objetos em quarentena. O Controle de dispositivo permite monitorar e restringir o acesso a dispositivos gerenciados através de conexões de rede e de dispositivos de E/S.

A tabela abaixo como as ferramentas do Security Suite complementam umas às outras e proporcionam uma defesa de sistema forte:

Preocupação / tarefa de segurança	Solução LANDesk Security Suite
Conhecimento e verificação	Modos de exibição do console: • Listas de conteúdo de segurança • Propriedades da definição (e regra de detecção) • Resultados da análise de Patch e conformidade • Atividades do antivírus e informações de status Alertas Relatórios
Gerenciamento de patches:	Patch e conformidade

Preocupação / tarefa de segurança	Solução LANDesk Security Suite
	Atualizações LANDesk Atualizações de drivers Atualizações de software
Avaliação e correção de vulnerabilidade (definições conhecidas publicadas no setor, definições personalizadas de segurança)	Patch e conformidade Download de definições e de arquivos de patch Análises de segurança Análises de conformidade distribuição e instalação do Patch Reparo automática
Detecção e reparo de malware	Antivírus • Atualizações e análise de arquivos padrão do LANDesk Antivirus • Atualizações do conteúdo de antivírus de terceiros Análises de Spyware Análises de Riskware Análises de Real-time Bloqueador de aplicativos
Configuração de dispositivo, proteção contra ataques dia zero e travamento	Segurança de ponto final • Alerta ao local (controle de conexão de rede) • Host Intrusion Prevention System (HIPS) • LANDesk Firewall • Controle de dispositivo • Listas de arquivos confiáveis Ameaças de segurança (exposições de configuração de sistemas) Configuração do Firewall do Windows: Agente Watcher
Controle de acesso de rede (autenticação, conformidade com diretiva de segurança)	Implementação do suporte ao LANDesk 802.1x NAC
Data Protection (criptografia inteligente baseada em diretivas)	LANDesk Data Protection mais Credant
Análise e descoberta de dispositivo não gerenciado	Descoberta de dispositivos não gerenciados

Preocupação / tarefa de segurança	Solução LANDesk Security Suite
	Descoberta de dispositivos estendida (ARP e WAP)

Após instalar o LANDesk Security Suite e ativar o servidor núcleo com a licença do Security Suite, você pode consultar as seções desse guia para inteirar-se das informações sobre a inicialização do console e o uso das ferramentas disponíveis, que incluem as ferramentas específicas de segurança e os recursos relacionados abaixo.

Navegar nos tópicos de ajuda do LANDesk Management Suite e LANDesk Security Suite no Central de ajuda LANDesk ou realize uma busca usando uma palavra-chave ou frase para encontrar a informação que você deseja.

IMPORTANTE: O Management Suite não inclui todos os componentes do Management Suite
Lembre-se de que alguns componentes do Management Suite não se aplicam à implementação do Security Suite como, distribuição de SO e núcleos rollup.

Instalar e ativar o LANDesk Security Suite

O LANDesk Security Suite e o LANDesk Management Suite, ambos, usam o mesmo programa de configuração para instalar os componentes necessários no seu servidor núcleo. A exemplo dos outros produtos de software da LANDesk como, Management Suite e o Inventory Manager, é no momento em que o servidor núcleo é ativado com as informações de conta da LANDesk, que a funcionalidade aplicável do Security Suite torna-se disponível no console.

Se a sua conta tiver licença para LANDesk Security Suite, você verá as ferramentas e os recursos descritos nos tópicos de ajuda do LANDesk Security Suite quando acessar o console.

Recursos do LANDesk User Community

Instalar e distribuir um aplicativo empresarial como os os softwares de soluções de segurança e sistemas da LANDesk em uma rede heterogênea, requer uma metodologia deliberada e um planejamento significativo antes da execução do programa de instalação.

Por serem similares, a infraestrutura da rede e os requisitos e considerações de escalonabilidade do banco de dados, e porque esses produtos LANDesk usa o mesmo programa de instalação, você deve consultar os documentos*Melhor método conhecido (BKM) de Instalação e Distribuição,* localizados na Comunidade de usuários da LANDesk.

NOTA: A Comunidade de usuários da LANDesk
A Comunidade de usuários LANDesk tem fóruns de usuários e os melhores métodos conhecidos para todos os produtos e tecnologia da LANDesk. Para acessar esse recurso valioso, visite: Página inicial da Comunidade de usuários da LANDesk

A Comunidade de usuários oferece vários documentos úteis que fornecem informações detalhadas sobre estratégias de distribuição em cada fase da distribuição de seus softwares LANDesk, como:

- Desenvolvimento do domínio de gerenciamento
- Preparação do banco de dados
- Instalar ou atualizar o servidor núcleo da LANDesk

- Entendendo o uso de portas
- Configure agentes de dispositivos gerenciados

Assinaturas do conteúdo do LANDesk Security Suite

O LANDesk Security Suite oferece suporte de análise e correção para vários tipos de riscos de segurança, que incluem as vulnerabilidades conhecidas de SO e aplicativo para plataformas suportadas de dispositivos, spyware, vírus, ameaças a configurações de sistemas, aplicativos não autorizados e mais. Cada risco de segurança, de qualquer tipo, é caracterizado por arquivos de definição. Um arquivo de definições é composto, em geral, de um ID, atributos específicos, detalhes de regra de detecção e informações de arquivo de patch, se aplicável.

O LANDesk mantém um banco de dados de arquivos de definição de segurança validados, conhecido como conteúdo de segurança ou conteúdo de segurança e patch, o qual é atualizado de forma contínua e está disponível para download através da Web. Para fazer download do conteúdo de segurança e patch é necessário ter uma assinatura de conteúdo do Security Suite.

Para obter informações sobre assinaturas de conteúdo, entre em contato com o representante da LANDesk ou visite o site da LANDesk:

LANDesk Home Page

Download de atualizações de segurança da LANDesk

A seção Patch e conformidade neste guia descreve como obter por download o conteúdo do segurança e patch para as assinaturas que você possui. Para obter mais informações, consulte "Download das atualizações do conteúdo de segurança" na página 571.

Tópicos relacionados

"Ferramentas e recursos do Security Suite" na página 503

Ferramentas e recursos do Security Suite

A ferramenta respectiva do LANDesk Security Suite é chamada Patch e conformidade. Para saber mais sobre o conteúdo de segurança e as plataformas suportadas de dispositivos, como usar o Patch e conformidade para executar uma análise e correção de segurança, ver resultados de análises, gerar relatórios de segurança e configurar a segurança contínua do sistema, consulte "Patch e conformidade" na página 549.

Este tópico de ajuda inclui vistas gerais breves das seguintes ferramentas de gerência de segurança fornecidos pelo LANDesk Security Suite, com conexões ao tópico de vista geral da ferramenta:

- "Patch e conformidade" na página 504
- "Conformidade com a convenção de nomes CVE" na página 504
- "Padrões Federais de Conformidade de Configuração do Desktop Núcleo (FDCC)" na página 505
- "Atividade de segurança" na página 505
- "Configurações do agente" na página 505

- "Segurança de ponto final" na página 505
  - "Visão geral do Host Intrusion Prevention System (HIPS)" na página 681
  - "Configurar parâmetros de firewall LANDesk" na página 695
  - "Controle de dispositivo" na página 700
  - "Na página Segurança de terminais: Página de diretivas do local" na página 680
- "LANDesk Antivirus" na página 506
- "LANDesk 802.1X NAC" na página 507
- "LANDesk Data Protection mais Credant" na página 507
- "Ferramentas comuns da LANDesk com Security Suite" na página 507
- "Outras características do LANDesk Management Suite com Security Suite" na página 509
- "Onde obter mais informações" na página 510

Patch e conformidade

Use o Patch e conformidade para fazer download das definições de vulnerabilidades conhecidas mais recentes (e outras definições de tipos de conteúdo de segurança) e os respectivos patches. Analisa dispositivos gerenciados assim como servidores núcleo e consoles, para as atualizações de software LANDesk. Configure e execute análises de avaliação de segurança personalizados para vulnerabilidades específicas de plataforma conhecidas, spyware, ameaças de segurança de configuração do sistema, analisadores de antivírus e aplicativos bloqueados ou aplicativos não autorizados.

Com a ferramenta de Patch e conformidade, você pode também:

- Cria também as suas próprias definições personalizadas de segurança para analisar dispositivos para condições específicas e de ameaças potenciais.
- Pesquisa, prioriza, descarrega e distribui e instala patches.
- Cria e executa tarefas agendadas e diretivas que corrigem os riscos de segurança detectados.
- Configure a análise de segurança para ser vista ou não nos dispositivos do usuário final durante a análise e processos de reparo, opções de reinicialização de dispositivo, e o nível de interação do usuário.
- Exibe informações abrangentes de segurança e patch para os dispositivos analisados.
- Habilitar alertas de segurança.
- Gera relatórios de segurança.

Para mais informações, veja "Patch e conformidade" na página 549.

NOTA: Análises de patch e conformidade em uma implementação do LANDesk Management Suite
A ferramenta de Patch e conformidade é incluído por padrão em uma instalação LANDesk Management Suite (ativação do servidor núcleo). Entretanto, no começo você só pode procurar atualizações de software LANDesk e as suas próprias definições personalizadas de segurança. Para analisar e corrigir tipos adicionais de segurança é necessário obter uma assinatura correspondente de conteúdo do Security Suite.

Conformidade com a convenção de nomes CVE

Produtos da LANDesk Security Suite suporta a convenção de nomes CVE (Common Vulnerabilities and Exposures). Com o Patch e conformidade você pode procurar vulnerabilidades por nomes CVE e ver as informações CVE das definições de vulnerabilidades das quais foi feito download.

Para obter mais informações sobre a convenção de nomes CVE, compatibilidade da LANDesk com o padrão CVE e saber como usar a identificação CVE para encontrar vulnerabilidades individuais em Patch e conformidade, consulte "Procurar vulnerabilidades por nomes CVE" na página 576.

Padrões Federais de Conformidade de Configuração do Desktop Núcleo (FDCC)

O LANDesk Security Suite apóia a iniciativa dos Padrões Federais de Conformidade de Configuração do Desktop Núcleo (FDCC) Os produtos de software LANDesk foram certificados pelo National Institute of Standards and Technology (NIST) em conformidade com os padrões Security Content Automation Protocol (SCAP) e estão listados como produtos validados no site do National Vulnerability Database.

Para realizar a análise de segurança FDCC e as tarefas de reparo, você deve ter uma assinatura de conteúdo LANDesk Security Suite que permita que você baixe o conteúdo específico do FDCC, que inclui: Detecção e instalação do analisador FDCC; elaboração de relatórios de status e conformidade FDCC e análise de vulnerabilidades e reparo certificados FDCC por componente.

Com o analisador certificado FDCC e o conteúdo de segurança, você pode analisar os dispositivos gerenciados para assegurar a conformidade com os padrões e requisitos Federais de Configuração do Desktop Núcleo.

Para obter mais informações sobre como usar o analisador e conteúdo de segurança FDCC, consulte "Visão geral dos padrões FDCC de conformidade" na página 616.

Atividade de segurança

A ferramenta Atividade de segurança lhe permite ver atividades críticas e informações de status de vários componentes de segurança e dispositivos. A Atividade de segurança fornece uma janela de ferramenta única onde você pode facilmente ver os resultados da análise do LANDesk Antivirus, prevenções do HIPS, prevenções do Firewall, dispositivos bloqueados do Controle de dispositivos e muito mais.

Para mais informações, consulte "Atividade da segurança" na página 668.

Configurações do agente

A ferramenta Configurações de agente lhe permite criar e gerenciar arquivos de configurações para vários componentes de segurança e dispositivos. Configurações (isto é, arquivos de configurações) controlam o modo como os serviços de segurança operam em dispositivos gerenciados.

Com a ferramenta Configurações de agente você pode distribuir agente/serviços e as configurações associadas para seus dispositivos gerenciados como parte da configuração de agente inicial, instalação separada ou tarefas de atualização e tarefas de configurações mudanças.

Para obter mais informações, consulte "Configurações de segurança" na página 656.

Segurança de ponto final

A nova ferramenta de Segurança de ponto final protege seus dispositivos gerenciados de ataques tipo dia zero, intrusões de firewall, aplicativos, ações e comportamentos de processos proibidos e conexões de rede e dispositivos não autorizadas.

A Segurança de ponto final é composta de arquivos de definições personalizados (configurações de recurso e opção salvos) que podem ser distribuídos a dispositivos alvo para esses componentes de segurança:

- Alerta ao local (controle de conexão de rede através de locais confiáveis)
- Host Intrusion Prevention System (HIPS)

- LANDesk Firewall
- Controle de dispositivo
- Listas de arquivos confiáveis

Host Intrusion Prevention System (HIPS)

O LANDesk Host Intrusion Prevention System (HIPS) fornece uma camada adicional de proteção preventiva para sistemas e aplicativos contra ataques zero-day (por exemplo, comportamento malicioso não autorizado). Ao usar regras personalizadas e certificações de arquivos, o HIPS monitora continuamente os processos especificados, arquivos, aplicativos e chaves de registro, além de bloquear ações e comportamentos proibidos. Com o HIPS você pode controlar quais aplicativos podem ser executados nos dispositivos e como são suas permissões de execução. HIPS permite que proteja o sistema de arquivos, registro, inicialização do sistema e até mesmo a detecção de kits de usuário raiz disfarçados.

Como o HIPS é um sistema baseado em regras e não um sistema baseados em definições (por exemplo, baseado em assinatura), como vulnerabilidade conhecida, spyware e análise antivírus, ele não precisa de atualizações constantes de arquivos. Você configura e distribui seu próprio nível personalizado de segurança de sistema.

Para obter mais informações, consulte "Visão geral do Host Intrusion Prevention System (HIPS)" na página 681.

LANDesk Firewall

O LANDesk Firewall lhe permite criar e configurar definições de firewall proprietárias para impedir o comportamento não autorizado de um aplicativo nos dispositivos gerenciados.

IMPORTANTE: Compatibilidade entre o LANDesk Firewall e Firewall do Windows
O Firewall da LANDesk complementa o Firewall do Windows e ambos podem ser habilitados e serem executados ao mesmo tempo nos dispositivos gerenciados.

Para obter mais informações, consulte "Configurar parâmetros de firewall LANDesk" na página 695.)

Controle de dispositivo

O Controle de dispositivo adiciona outro nível de segurança à sua rede LANDesk ao permitir a monitoração e o acesso restrito a dispositivos gerenciados através de dispositivos de E/S. Com o Controle de dispositivo você pode restringir o uso de dispositivos que permitem acesso de dados a dispositivos como portas, modem, unidades de disco, dispositivos USB e conexões sem fio.

Para mais informações, consulte "Controle de dispositivo" na página 700.

LANDesk Antivirus

O LANDesk Antivirus permite proteger todos os dispositivos gerenciados contra os vírus mais recentes conhecidos, assim como suspeitas de infecção. As análises de antivírus podem também verificar se há riskware (através de um banco de dados estendido). O LANDesk Antivirus é uma ferramenta configurável de proteção de vírus completamente integrada com LANDesk Security Suite e LANDesk Management Suite.

O LANDesk Antivirus fornece uma gama ampla de recursos antivírus, incluindo o seguinte: análises agendadas antivírus, análises por demanda, análise de botão vermelho, proteção de arquivo e e-mail em tempo real, download automatizado de atualizações de arquivos de definição (o banco de dados de assinaturas de vírus da LANDesk contém as definições conhecidas de vírus mais recentes e é atualizado várias vezes ao dia), configuração de comportamento de análise antivírus e opções de usuário final, exclusões de análise, assim como alertas e relatórios de antivírus.

Além disso, você pode ver informações sobre antivírus em tempo real de dispositivos analisados no console principal e no Painel executivo baseado no Web console para identificar rapidamente ataques de vírus e ver o controle de vírus por um período especificado.

Para mais informações, consulte "LANDesk Antivirus" na página 712.

LANDesk 802.1X NAC

Use o NAC (Network Access Control) para implementar a segurança de conformidade na rede. O suporte ao LANDesk 802.1X NAC foi criada para estender a segurança de uma implementação de servidor Radius 802.1X existente na sua rede ao adicionar a autenticação e conformidade.

O 802.1X NAC permite a configuração personalizada de diretivas de segurança de conformidade com o uso da ferramenta Patch e conformidade e aplica essas diretivas nos dispositivos que tentam acessar a rede através de um processo de validação de postura. Os dispositivos em estado de funcionamento recebem direito de acesso e os dispositivos fora de funcionamento são colocados em quarentena, onde podem ser corrigidos e receber direito de acesso pleno ou receber direito de acesso limitado à rede. Você pode também criar e configurar análises de segurança específicas de conformidade que verificam os dispositivos conectados no momento para conformidade a sua diretiva de segurança. As análises completas de segurança de conformidade podem ser iniciadas por uma análise antivírus quando não for possível remover ou colocar um vírus em quarentena.

IMPORTANTE: O LANDesk NAC requer configuração adicional de hardware e software e um forte conhecimento prático de autenticação de servidor Radius 802.1X, autenticação de 802.1X e validação de postura de funcionamento assim como princípios de design de infra-estrutura de rede avançada e administração.

Para mais informações, consulte "Visão geral da ferramenta LANDesk 802.1X NAC" na página 517.

LANDesk Data Protection mais Credant

Ferramentas comuns da LANDesk com Security Suite

As ferramentas comuns da LANDesk fornecem a configuração respectiva do dispositivo e capacidades de gerenciamento em Management Suite e Security Suite. As seguintes ferramentas estão disponíveis em uma LANDesk Security Suite implementação, aparecendo no menu **Ferramentas** no console.

IMPORTANTE: Observe que algumas dessas ferramentas comuns têm certas restrições em uma licença de ativação do LANDesk Security Suite.

Configuração de agente

Use a Configuração de agentes para criar configurações personalizadas de agente para distribuição e instalação dos agentes LANDesk necessários, requeridos para o gerenciamento e proteção dos dispositivos da sua rede. Esses são agentes LANDesk padrão (que incluem analisador de inventário, planejador local, detecção de banda larga e análise de segurança), além do agente de distribuição de software e o agente de monitoração de licença de software (usado para bloquear aplicativos).

NOTA: Agentes não aplicáveis a LANDesk Security Suite
Os seguintes agentes de LANDesk (componentes) NÃO são aplicáveis em uma Security Suite instalação:
- Formulários de dados personalizados
- controle remoto
- distribuição de SO

Relatórios

Use a ferramenta Relatórios para gerar e publicar uma grande variedade de relatórios especializados que oferecem informações úteis sobre os seus dispositivos gerenciados, incluindo vários relatórios pré-definidos do Patch e conformidade, Antivirus e LANDesk NAC Compliance.

NOTA: Relatórios não aplicáveis aoLANDesk Security Suite
As seguintes categorias de relatórios NÃO se aplicam ao Security Suite: Todos os Relatórios de recursos, Todos os relatórios SLM e Todos os relatórios de controle remoto.

Tarefas agendadas

Use as Tarefas agendadas para criar tarefas recorrentes especialmente relacionadas ao gerenciamento de segurança e patch, reparo, cumprimento de segurança de conformidade, análise antivírus, entre outros. Você pode configurar os dispositivos alvo da tarefa e as opções de agendamento.

NOTA: Tarefas agendadas não aplicáveis ao LANDesk Security Suite
Os seguintes tipos de tarefas agendadas (script) NÃO se aplicam ao Security Suite: Formulários de dados personalizados, Scripts personalizados, Tarefas de dispositivos portáteis e scripts de OSD. Além disso, o pacote de distribuição e as opções de método de distribuição não são configuráveis através do Security Suite.

Descoberta de dispositivos não gerenciados

Use a Descoberta de dispositivos não gerenciados (UDD) para localizar dispositivos na sua rede, os quais não enviaram uma análise de inventário ao banco de dados núcleo.

A descoberta de dispositivos estendida (XDD) funciona fora dos métodos de descoberta usados pela UDD. Os dispositivos gerenciados com o agente de descoberta estendida de dispositivo estão alertas para difusões ARP (Protocolo de resolução de endereço) e mantêm um cache (na memória e em um arquivo na unidade local) dos dispositivos que as fazem. A descoberta estendida de dispositivo pode, também, detectar dispositivos WAP (ponto de acesso sem fio).

Administração com base em funções

A ferramenta Gerenciamento de usuário permite adicionar usuários a funções de gerenciamento do Security Suite e configurar os respectivos acessos a ferramentas específicas e gerenciar dispositivos baseado em suas funções administrativas.

Com a administração com base em funções, você atribui funções (com os direitos associados) para determinar as tarefas que os usuários podem executar além de escopos (com base em grupos de dispositivos, consultas, diretórios LDAP ou diretórios personalizado) para para determinar os dispositivos que um usuário pode ver e gerenciar. Os funções com Security Suite que estão disponível incluem: Patch e conformidade, Controle de acesso de rede, Configurações de agente, Distribuição de software, Gerenciamento de consulta pública e Descoberta de dispositivo não gerenciado.

NOTA: As funções e direitos não aplicáveis a LANDesk Security Suite
Os seguintes direitos de administração baseada em funções NÃO são aplicáveis ao Security Suite: Distribuição de SO, Controle remoto, Configuração de recursos, Entrada de dados de recursos e Monitoração de licença de software.

Contas locais

Contas locais é uma ferramenta administrativa usada para gerenciar os usuários e grupos nos computadores locais na sua rede. Através do console, é possível adicionar e excluir usuários e grupos, adicionar e remover usuários de grupos, definir e mudar senhas, editar configurações de usuário e grupo, e criar tarefas para reconfigurar senhas de vários dispositivos.

Outras características do LANDesk Management Suite com Security Suite

Além das ferramentas mencionadas acima e que são exibidas no menu Ferramentas do console, o Security Suite fornece os seguintes recursos comuns LANDesk:

- Console do Windows, consoles adicionais, Web console
- Layouts de console personalizados
- Tela de rede para dispositivos gerenciados e consultas
- Menus de atalho para dispositivos gerenciados e consultas
- Configuração de serviços
- Inventário
- Consultas de banco de dados
- Distribuição de software
- Monitoração de licenças de software
- Alertas
- Replicação de conteúdo e servidores preferenciais

IMPORTANTE: Os formulários de dados personalizados não são suportados no LANDesk Security Suite
Os formulários de dados personalizados não estão disponíveis na licença de apenas LANDesk Security Suite. É necessário uma licença completa do LANDesk Management Suite a fim de usar o recurso de

formulários de dados personalizados.

Onde obter mais informações

Seguir os tópicos de ajuda de ferramenta de segurança, a sobra dos tópicos ligados de ajuda são achados nas LANDesk Management Suite seções de ajuda que cobrem as ferramentas comuns de LANDesk mencionados acima (inclusive informações sobre entendimento e usar o console e tela de rede).

NOTA: A Comunidade de usuários da LANDesk
A comunidade de usuários da LANDesk tem fóruns de usuários e os melhores métodos conhecidos para todos os produtos e tecnologias LANDesk. Para acessar esse recurso valioso, visite: Página inicial da Comunidade de usuários da LANDesk

Tópicos relacionados

"Introdução ao LANDesk Security Suite" na página 500

Controle de acesso à rede (NAC)

Visão geral do LANDesk NAC

NAC (Network Access Control - Controle de acesso de rede) é um componente importante de uma solução de gerenciamento de segurança abrangente. O NAC protege a sua rede de acesso não autorizado, intrusões fraudulentas e exposições externas de segurança introduzidas por dispositivos vulneráveis ou corrompidos que podem infectar e danificar sua rede.

O LANDesk Security Suite oferece a ferramenta 802.1X NAC criada para suportar e estender a segurança de uma implementação de servidor Radius 802.1X existente na sua rede. O suporte para LANDesk 802.1X NAC adiciona recursos de autenticação e conformidade para funcionalidade de controle de acesso básico de 802.1X.

NOTA: A Comunidade de usuários da LANDesk
A Comunidade de usuários LANDesk tem fóruns de usuários e os melhores métodos conhecidos para todos os produtos e tecnologia da LANDesk. Para acessar esse recurso valioso, visite: http://community.landesk.com

O NAC (Network Access Control - Controle de acesso de rede) adiciona uma camada extra de proteção a sua rede, que permite impedir os dispositivos vulneráveis e corrompidos de ganharem acesso à rede e também protege os recursos críticos da rede contra sistemas conectados que se tornam corrompidos.

O NAC estabelece uma segurança de perímetro de ponto final usando as tecnologias de segurança e sistemas de segurança padrão da indústria. O NAC (Network Access Control - Controle de acesso de rede) fornece flexibilidade na implementação da funcionalidade de controle de acesso de rede na sua rede através do suporte aos padrões e as metodologias comuns da indústria, como o IEEE 802.1X.

Com o NAC, você pode definir diretivas personalizadas de segurança de base, analisar dispositivos (gerenciados e não gerenciados) para verificar a conformidade de segurança, verificar status de funcionamento (postura) de dispositivos que estão conectando e negar ou permitir acesso aos seus recursos críticos de rede com base na conformidade do dispositivo com a diretiva de segurança. Os dispositivos em bom funcionamento recebem acesso total à rede. Se for determinado que um dispositivo está em estado de não funcionamento, ele será impedido de acessar a rede e permanecerá em uma zona de quarentena virtual onde poderá ser reparado com os recursos de correção do Security Suite ou será permitido acesso limitado à rede.

Com o NAC, também é possível avaliar as credenciais de segurança de qualquer dispositivo assim que ele tentar conectar-se à rede comparando-o com as diretivas de segurança personalizadas, monitorar o estado de segurança de dispositivos que já estão conectados, permitir ou negar acesso à rede, colocar em quarentena os dispositivos que não satisfazem os requisitos da diretiva de segurança e corrigir dispositivos vulneráveis para que eles possam ser reanalisados a fim de verificar a conformidade com a diretiva de segurança e receberem acesso à rede assim que forem considerados em bom funcionamento.

Benefícios e recursos do NAC (Network Acess Control - Controle de acesso à rede)

Com o NAC é possível:

- Criar e fazer cumprir as diretivas de conformidade de segurança
- Implementar a segurança de empresa mais forte e contínua
- Acessar as credenciais de segurança (estado de funcionamento) de dispositivos que se conectam
- Impedir sistemas infectados ou corrompidos de acessarem a rede
- Por em quarentena os dispositivos fora de conformidade em uma área segura
- Corrigir dispositivos infectados para colocá-los dentro da conformidade
- Reduzir tempo ocioso devido a infecções de intrusões fraudulentas
- Proteger a rede, sistemas, aplicativos e dados de ameaças externas
- Estender as tecnologias e padrões de segurança existentes

Diretivas de segurança de conformidade

As diretivas de segurança de conformidade são compostas de regras que verificam o estado de funcionamento de um dispositivo verificando vulnerabilidades (na forma de patches ausentes ou obsoletos do SO e do aplicativo), atualizações de software, arquivos de mecanismo de assinatura de antivírus, presença e configurações de firewall e spyware.

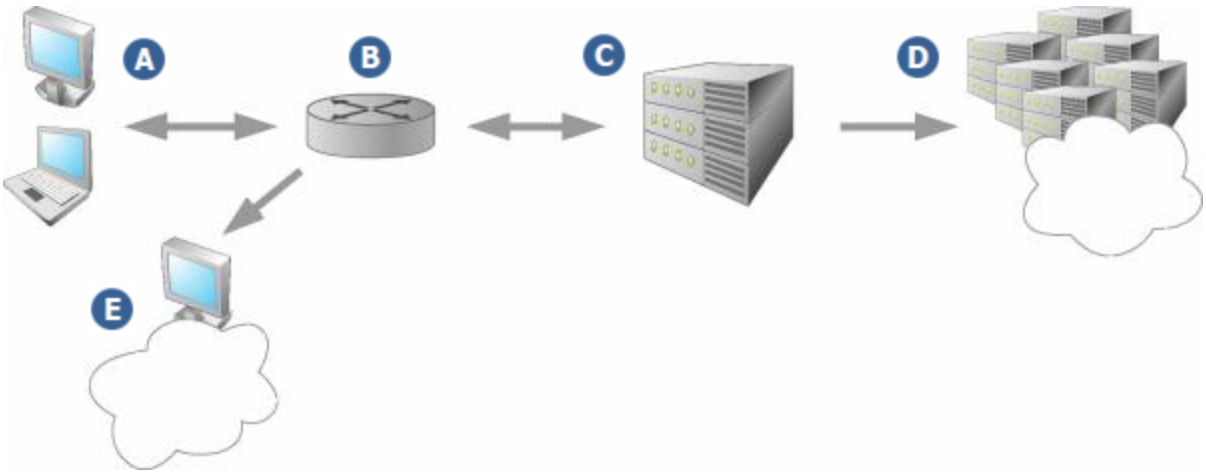
Para obter mais informações sobre a definição da diretiva de segurança de conformidade na Ferramenta de Patch e conformidade no console, consulte "Definir critérios de segurança de conformidade na ferramenta Patch e conformidade" na página 536.

Entenda os componentes básicos do NAC

As seções abaixo descrevem os componentes básicos de uma implementação do NAC (do inglês, Network Access Control) e a função de cada componente e como eles interagem.

Componentes NAC básicos e fluxo de processo

O diagrama abaixo exibe os componentes NAC básicos, suas funções e o fluxo de comunicação entre as diversas peças.



***A** Dispositivos tentando acessar a rede, **B** Dispositivo de controle e acesso à rede, **C** Ponto de decisão de acesso de rede / servidor de diretiva, **D** Rede corporativa, **E** Quarentena VLAN*

Descrições básicas dos componentes NAC

Componente	Descrição
A: Dispositivos tentando acessar a rede	Inclui as conexões ocasionais ou dispositivos portáteis, visitantes e usuários convidados assim como os usuários regulares da rede tentando acessar a rede corporativa. Os dispositivos com agente confiável instalado podem comunicar-se com o servidor de diretiva ou de validação de postura a fim de enviar e receber informações sobre credenciais de funcionamento e podem ser reparados pelo servidor de correção se forem detectadas vulnerabilidades durante a análise de segurança. Sem um agente confiável, o dispositivo não pode comunicar-se com o servidor de validação de postura e não pode ser corrigido. Quando um dispositivo sem o agente de confiança é analisado pela primeira vez, o dispositivo é direcionado para uma página da Web com links para instalar o agente de confiança apropriado.
B: Dispositivo de controle de acesso à rede	O dispositivo de controle de acesso à rede funciona como o dispositivo de rede de "primeiro salto" (first hop) do ponto de vista do dispositivo solicitante que inicia a validação de postura e autenticação.
C: Diretiva do servidor/servidor de validação de postura (ponto de decisão de acesso à rede)	Um servidor back-end dedicado também conhecido como o servidor de validação de postura que avalia as credenciais de postura (estado de dispositivos que solicitam acesso) com base nas regras de conformidade (diretiva de segurança nele publicadas pelo servidor núcleo). Envia uma resposta de validação (funcionamento, não funcionamento, etc.) através do dispositivo de controle de acesso à rede.
D: Rede corporativa	Área e recursos críticos de rede protegidos pelo NAC contra dispositivos fora de funcionamento, infectados ou vulneráveis.
E: VLAN de quarentena	Área de rede virtual segura onde os dispositivos fora de conformidade podem ser colocados e corrigidos, analisados novamente e receber acesso total ou retidos com acesso restrito, por exemplo, acesso à Internet.

Pré-requisitos NAC e direitos RBA

Para usar o recurso NAC, é necessário ter uma licença válida do Security Suite (ativação do servidor núcleo).

O LANDesk requer não apenas os recursos de análise e correção da ferramenta Patch e conformidade, mas também as assinaturas de conteúdo do Security Suite para o download de vulnerabilidades, spyware, ameaças de configuração do sistema e arquivos de definições de vírus que são usados para criar os critérios e regras de conformidade personalizados ou diretivas de segurança.

Foi adicionado um grupo denominado Conformidade à tela de árvore de grupos do Patch e conformidade. Os usuários com o direito de Patch e conformidade podem adicionar e remover definições de tipo de segurança do grupo Conformidade. As definições de segurança contidas no grupo Conformidade constituem a diretiva de segurança de conformidade e são verificadas por análise nos dispositivos que se conectam a fim de determinar seu estado de funcionamento.

Administração com base em funções com o LANDesk 802.1X NAC

O NAC (Network Access Control) depende dos seguintes direiso baseados em funções.

Direito de Patch e conformidade

Este direito é necessário para ver e acessar a ferramenta Patch e conformidade e fazer download das atualizações de conteúdo de segurança necessárias para definir as regras de conformidade. Este direito é necessário para adicionar e remover definições de segurança do grupo Conformidade.

Direito de Administrador

Este direito é necessário para configurar dispositivos com os agentes confiáveis para análise de conformidade e para configurar serviços NAC no console.

NOTA: A permissão de Administrador inclui todos as permissões, incluindo os dois direitos relacionados a segurança mencionados acima.

Lista de tarefa de início rápido para a configuração de uma implementação LANDesk 802.1X NAC

Use esta lista de tarefas para o planejamento, instalação e configuração de tarefas necessárias para a implementação do suporte a 802.1X NAC na sua rede.

Imprima esta lista de tarefas e use-a para acompanhar cada etapa durante o processo de implementação. Se estiver utilizando esta lista de tarefas online, clique no link **Para mais informações** para ver as informações detalhadas sobre uma tarefa em particular.

Terminado	Tarefa	Para ver mais informações, vá para
	Pré-requisito: Deve haver um servidor núcleo instalado, funcionando na rede e ativado com uma licença do Security Suite e assinaturas de conteúdo de segurança: • Instalação do servidor núcleo • Ative o núcleo com uma licença do Security Suite • Acesse como um usuário Administrador ou como usuário com direitos de Segurança (permite descarregar conteúdo de segurança e copiá-lo no grupo Conformidade)	Para obter mais informações sobre o uso da ferramenta Patch e conformidade, consulte "Patch e conformidade" na página 549. Para obter informações sobre os componentes e o fluxo de trabalho do 802.1X NAC, consulte "Visão geral da ferramenta LANDesk 802.1X NAC" na página 517. Para obter mais

Terminado	Tarefa	Para ver mais informações, vá para
		informações sobre topologia de rede e considerações sobre design para a implantação do 802.1X NAC, consulte "Visão geral da ferramenta LANDesk 802.1X NAC" na página 517.
	Instalação de um servidor de correção: • Em um computador servidor diferente, • Execute o script de configuração CONFIGURE.REMEDIATION.SERVER.VBS localizado em: <coreserver>\LDMain\Install\TrustedAccess\RemediationServer • **NOTA:** Este script configura automaticamente o servidor o servidor para executar a correção, fazendo o seguinte: • criando um compartilhamento de Web denominado LDLogon (tipicamente) no diretório: c:\inetpub\wwwroot\LDLogon) • habilitando o acesso anônimo ao compartilhamento LDLogon com direitos de Leitura e Procura • adicionando um novo tipo de MIME para .lrd e definindo-o para aplicativo/octeto-fluxo	"Instalar e configurar um servidor de correção" na página 532
	Configure (adicione) o servidor de correção no console: • Na janela da ferramenta de **Controle de acesso de rede**, clique com o botão direito no objeto **802.1X** e clique em **Configurar 802.1X** e, a seguir, clique em **Servidores de correção** e clique em **Adicionar** • Digite o endereço IP do servidor de correção, o caminho UNC para o compartilhamento de web LDLogon que criou no servidor de correção os arquivos são publicados, as credenciais de acesso do usuário e clique em **OK**	"Instalar e configurar um servidor de correção" na página 532
	Publique as configurações do NAC para os servidores de correção: • Em **Controle de acesso de rede**, clique com o botão direito em **802.1X**, clique em **Publicar configurações do NAC**, selecione **Todos** e clique em **OK** • **NOTA:** O processo de publicação inicial deve incluir TODAS as configurações do NAC; as publicações subseqüentes podem incluir somente o conteúdo de conformidade	"Publicar as configurações de NAC em servidores" na página 538
	Defina critérios de segurança de conformidade com a ferramenta Patch e conformidade	"Definir critérios de segurança de conformidade na ferramenta Patch e conformidade" na página 536

Terminado	Tarefa	Para ver mais informações, vá para
	• Na ferramenta **Patch e conformidade** do console, • Descarregue as definições de conteúdo de segurança e patches • Adicione definições ao grupo **Conformidade** para definir a sua diretiva de segurança de conformidade • Verifique se os patches associados foram descarregados e estão disponíveis para distribuição • Crie uma configuração de conformidade que aplique as análises compatíveis com 802.1X • (A diretiva de segurança de conformidade do 802.1X NAC é também definidad pelo parâmetro de tempo de quarentena automática na configuração de agente do dispositivo.)	
	Habilite o suporte a 802.1X NAC e configure o servidor Radius 802.1X ou proxy no console: • Em **Controle de acesso de rede**, clique em **802.1X**, clique em **Configurar 802.1X**, clique em **Servidor Radius**, e primeiro verifique se a opção **Habilitar servidor Radius 802.1X** está selecionada, selecione o tipo EAP e, a seguir, selecione o uso do plug-in LTA EAP IAS ou do proxy Radius LTA (requer a configuração de definições de proxy)	"Visão geral da ferramenta LANDesk 802.1X NAC" na página 517
	Instale o agente do 802.1x nos dispositivos gerenciados para habilitar a análise de conformidade (**NOTA:** Ao distribuir o agente do 802.1X, é necessário especificar o método de endereçamento da rede de quarentena para dispositivos com mau funcionamento. O endereçamento de quarentena pode ser feito por uma faixa de endereços IP ou por DHCP na rede de quarentena. Você configura esse esquema de endereçamento no roteador.) • **Para os dispositivos gerenciados de funcionários:** Se eles já tiverem o agente padrão LANDesk, habilite o suporte 802.1X com uma nova configuração de agente de dispositivo Ou, se eles não tiverem o agente padrão, habilite o suporte a 802.1X com a configuração inicial de agente Ou, habilite o suporte a 802.1X com uma configuração de agente para dispositivos em UDD • **Para dispositivos não gerenciados de funcionário:** Habilite o suporte a 802.1X por recepção com o agente padrão LANDesk (wscfg32.exe) Ou, com o uso de uma configuração de agente independente	"Visão geral da ferramenta LANDesk 802.1X NAC" na página 517
	Configure o seu switch de rede para autenticação, quarentena e correção de 802.1X: • Vá para o site de Suporte para ver as recomendações e os exemplos de configuração	"Visão geral da ferramenta LANDesk 802.1X NAC" na página 517
	Configure o seu roteador de rede para fornecer segurança entre a rede de produção e a rede de quarentena 802.1X:	"Visão geral da ferramenta LANDesk

Terminado	Tarefa	Para ver mais informações, vá para
	• Vá para o site de Suporte para ver as recomendações e os exemplos de configuração	802.1X NAC" na página 517
	Assegure-se de que o processo de autentição e validação de postura esteja funcionando corretamente: • Experimente fazer um teste simples de 802.1X NAC conectando um dispositivo configurado com suporte ao LANDesk 802.1X NAC à rede.	
	Execução das tarefas contínuas de gerenciamento de segurança de conformidade: • Verificar se o suporte ao 802.1X NAC está habilitado • O que acontece quando os dispositivos sendo conectados estão em postura • Como ver dispositivos fora de conformidade • Modificação e atualização de diretivas de segurança de conformidade • Adição de dispositivos não gerenciados • Como configurar e ver o login de conformidade	"Primeiro, verifique se o suporte ao 802.1X NAC está habilitado" na página 544

Para voltar para a seção principal do LANDesk 802.1X NAC, consulte "Visão geral da ferramenta LANDesk 802.1X NAC" na página 517.

Visão geral da ferramenta LANDesk 802.1X NAC

O LANDesk 802.1X NAC melhora o controle de acesso à rede ao exigir as credenciais corretas de autenticação e um agente padrão no dispositivo. Você pode também validar a conformidade de funcionamento do dispositivo com a sua diretiva de segurança personalizada e por em quarentena e corrigir dispositivos em mau funcionamento.

O LANDesk 802.1X NAC funciona com todos os principais fornecedores de switches que oferecem suporte ao padrão 802.1X. O proxy 802.1X Radius pode participar de uma arquitetura de gerenciamento de identidades AAA (autenticação, autorização e contabilidade) existente que autentica usuários e pontos finais, ou atuar como um Radius independente para ambientes que necessitam somente da validação de conformidade de pontos finais. As provisões do Radius Proxy alternam o acesso a portas com base nos resultados de autenticação para pontos finais conectados.

Essas seções descrevem, como planejar, configurar e habilitar o suporte ao LANDesk 802.1X NAC em um ambiente NAC existente.

A ferramenta LANDesk 802.1X NAC foi criada para suportar e estender a segurança de uma implementação de servidor Radius 802.1X existente na sua rede. O suporte para LANDesk 802.1X NAC adiciona recursos de autenticação e conformidade para funcionalidade de controle de acesso básico de 802.1X.

IMPORTANTE: Conhecimento técnico e experiência necessários para a configuração de NAC
Observe que o NAC requer a configuração adicional de hardware e software além da instalação básica do servidor núcleo. Por causa da natureza técnica deste trabalho de configuração adicional, A LANDesk

presume que você está familiarizado com a configuração do servidor Radius 802.1X, a autenticação de 802.1X e a validação de postura de funcionamento, além dos princípios de design e administração de infra-estrutura de rede avançada.

O que fazer após a configuração de suporte do LANDesk 802.1X NAC

Após concluir as tarefas de configuração indicadas acima, a próxima etapa na implementação do NAC é definir sua diretiva de segurança de conformidade, publicar as configurações do NAC para os servidores adequados e personalizar as páginas de correção HTML como desejado. Para obter mais informações, consulte "Definir critérios de segurança de conformidade na ferramenta Patch e conformidade" na página 536.

Outras tarefas de gerenciamento do NAC incluem: garantia da ativação dos serviços do 802.1X NAC através do uso da opção permitir/restringir acesso a todos, compreensão do que acontece quando os dispositivos sendo conectados estão em postura, atualização das regras e diretivas de segurança de conformidade e republicação de parâmetros do LANDesk NAC, acréscimo de dispositivos não gerenciados à ferramenta Descoberta de dispositivo não gerenciado, observação de dispositivos afetados configuração de acesso. Para obter mais informações, consulte "Primeiro, verifique se o suporte ao 802.1X NAC está habilitado" na página 544.

Consulte a lista de tarefas de início rápido

Para a sua conveniência, use esta lista de verificação de tarefa para ajudar a controlar as etapas requeridas na configuração do LANDesk 802.1X NAC: Veja a "Lista de tarefa de início rápido para a configuração de uma implementação LANDesk 802.1X NAC" na página 514.

Tecnologias LANDesk 802.1X NAC

O IEEE 802.1X é um protocolo de segurança IEEE usado no controle de acesso à rede com base em portas. O 802.1X fornece a autenticação para dispositivos, seja estabelecendo uma conexão ou impedindo o acesso em caso de falha na autenticação. O 802.1X é baseado em EAP (Extensible Authentication Protocol - Protocolo de autenticação extensível) e no mais recente PEAP (Protected Extensible Authentication Protocol - Protocolo de autenticação extensível protegida). é aceito pela maioria dos switches de rede e pode ser configurado para autenticar os clientes que possuem o software do agente instalado.

O controle de acesso à rede do 802.1X NAC é uma solução de autenticação e acesso de rede proxy Radius 802.1X que funciona com todos os principais fornecedores de switches de rede que suportam o padrão 802.1X. Com o servidor 802.1X NAC, um servidor Radius (um servidor Microsoft IAS com o plug-in LANDesk EAP IAS ou um servidor Radius com o proxy do 802.1X) executa validação de postura ou, em outras palavras, verifica a conformidade com a diretiva de segurança.

A autenticação padrão do 802.1X exige um nome de usuário e senha para acessar a rede. O LANDesk 802.1X NAC estende seu modelo básico solicitando também que o agente padrão (CBA) seja instalado nos dispositivos gerenciados que solicitam acesso à rede e o dispositivo suplicante é determinado como compatível com a diretiva de segurança personlizada. O NAC verifica a presença do agente LANDesk procurando por uma ID única de dispositivo criado pelo próprio agente. (Nota: O EAP não tentará fazer a autenticação se não encontrar o ID de dispositivo.)

O 802.1X NAC com o plug-in EAP IAS usa um agente proprietário do NAC EAP que reside tanto no servidor IAS Radius como nos dispositivos gerenciados. O agente LTA EAP é instalado nos dispositivos gerenciados através de uma programa de instalação de agente.

Além do componente específico de servidor Radius 802.1X e necessária configuração de switch e roteador, é necessário também configurar um servidor de correção a fim de implementar o Controle de acesso de rede.

Com 802.1X NAC, o servidor Radius age como o ponto de decisão de acesso de rede e funciona em conjunto com o switch de rede. O switch age como o dispositivo de controle de acesso de rede e encaminha as solicitações de autenticação de dispositivo para o servidor Radius que executa a autenticação real. Dependendo dos resultados devolvidos ao switch pelo servidor Radius, o switch concede ou nega o acesso dos dispositivos à rede.

Fluxos de processo, topologia de rede e componentes 802.1X NAC

Esta seção descreve os componentes que constituem a solução 802.1X NAC. Esta seção também explica o que acontece quando um dispositivo tenta acessar ou conectar-se à rede corporativa quando o NAC é ativado.

Os seguintes componentes são requeridos para LANDesk 802.1X NAC.

Componentes requeridos

Componente	Descrição
Servidor núcleo	Fornece a ferramenta Patch e conformidade usada para: Download do conteúdo de segurança (como definições de vulnerabilidade de SO e aplicativos, definições de spyware, etc.) Define critérios de conformidade Configura servidores de correção Configura a instalação de pacotes de instalação (MSI) de proxy de Radius Configura e publica as configurações de NAC (inclui diretivas de segurança de conformidade e recursos de correção para dispositivos de análise e reparo)
Plug-in de servidor Radius, Or proxy Radius	Age como ponto de decisão de acesso de rede. Use o plug-in de servidor 802.1X IAS se quiser utilizar um servidor IAS existente (ou configurar um novo servidor IAS). Use o método proxy Radius se tiver um servidor Radius além do IAS ou se quiser usar PEAP como o tio de EAP especificado.
Servidor de correção	Contém os arquivos necessários para configuração e suporte (definições de tipo de segurança e patchs necessários assim como as páginas de correção HTML usadas para analisar dispositivos para detectar vulnerabilidade) identificados pela sua diretiva de segurança. Corrige qualquer vulnerabilidade detectada para que o dispositivo possa ser analisado como em funcionamento ou compatível e acessar a rede.

Componente	Descrição
Switch	Age como o dispositivo de controle de acesso de rede e encaminha as solicitações de autenticação de dispositivo para o servidor Radius que executa a autenticação real.
Roteador	Age como um dispositivo de acesso à rede que faz cumprir a diretiva de segurança de conformidade. Comunica-se com ambos, o dispositivo sendo conectado e tentando o acesso e o servidor servidor Radius 802.1X para avaliar as credenciais de postura do dispositivo de ponto final. Em outras palavras, num ambiente 802.1X NAC o roteador é o ponto de fiscalização da diretiva na rede e concede ou nega privilégios de acesso.
Dispositivos	Dispositivos de usuários, que tentam acessar a sua rede corporativa. Dispositivos de ponto final típicos incluem computadores desktop e laptops, mas também os dispositivos sem clientes como impressoras. O NAC permite a você avaliar o status de funcionamento desses dispositivos conectados e restringir o acesso à rede com base em suas credenciais de postura.

Fluxo do processo 802.1X NAC

1. Um dispositivo gerenciado configurado com o agente LANDesk 802.1X faz uma tentativa inicial de acessar a rede corporativa.
2. O switch de rede (configurado para encaminhamento de passagem do 802.1X e atuando como ponto de controle de acesso) envia uma solicitação de identidade EAP para o dispositivo solicitante.
3. Um prompt aparece no dispositivo, solicitando nome de usuário e senha. O usuário final deve digitar as credenciais válidas de login, que são encaminhadas pelo switch, com um token adicionado ao pacote de resposta EAP, para o servidor Radius (configurado ou com um plug-in LTA EAP ou com o proxy Radius LTA, atuando como ponto de decisão de acesso).
4. Se as credenciais de autenticação são reconhecidas e o símbolo indicar que o dispositivo tem um agente padrão instalado, o LANDesk 802.1X NAC executa uma análise de segurança de conformidade que determina a postura do dispositivo ou o status de funcionamento de acordo com os critérios definidos pela sua diretiva de segurança personalizada. A análise é executada por uma tarefa de análise de conformidade, usando as configurações de conformidade que têm a opção **Reforçar análise do 802.1X** ativada na página **Conformidade**.
5. Se o dispositivo é considerado em bom funcionamento (ou em conformidade), ele recebe o acesso à rede corporativa
6. Se o dispositivo é considerado estar em mau funcionamento (ou fora de conformidade), ele permanece na quarentena VLAN. Uma caixa de diálogo é exibida informando ao usuário como entrar em contato com o servidor de correção para executar análises avaliação de vulnerabilidade e correção. O atalho de Correção é criado na área de trabalho do dispositivo. O usuário final, então, escolhe se quer permanecer na quarentena VLAN ou realizar as etapas necessárias para demonstrar conformidade com a diretiva de segurança e ganha pleno acesso à mesma.

7. A correção é feita pelo servidor de correção através da análise para verificar vulnerabilidades e outros risco à segurança (as regras de conformidade mencionadas acima) e através da instalação dos patches que forem necessários. Assim que o dispositivo estiver reparado, o processo de acesso à rede é repetido e o dispositivo, que agora está em bom funcionamento, recebe acesso à rede corporativa.

NOTA: Análises de segurança de conformidade
Com a ferramenta Patch e conformidade Manager, você pode criar e configurar uma análise de segurança específica de conformidade, que verifica a conformidade dos dispositivos alvo com a sua diretiva de segurança personalizada. Uma análise de conformidade é baseada no conteúdo do grupo Conformidade e pode ser executada como uma tarefa agendada ou uma diretiva. Para obter mais informações sobre a atualização de diretivas e regras de segurança de conformidade e sobre a republicação de parâmetros do NAC, consulte "Primeiro, verifique se o suporte ao 802.1X NAC está habilitado" na página 544.

Considerações de topologia de rede e design

Você deve mante as seguintes questões em mente ao implementar o suporte para o LANDesk 802.1X NAC em um ambiente de servidor Radius 802.1X existente.

- O **servidor de correção** e o **Servidor Radius** podem ser instalados no mesmo computador, mas se surgir problemas de desempenho ou escalonabilidade eles devem ser mudados para servidores separados.
- O **switch de rede** precisa ser configurado para encaminhamento de passagem de 802.1X.
- O roteador precisa ser configurado com duas subredes VLAN: a subrede primária é a rede corporativa/de produção; a secundária é a rede de quarentena (isto é, VLAN 802.1X convidada).
- A **rede de quarentena** do roteador deve usar listas de controle de acesso (ACL) para restringir o acesso de dispositivo a apenas o servidor de correção.
- O **servidor núcleo** não deve ser visível à rede de quarentena.

O fluxo de trabalho abaixo descreve o fluxo de comunicações entre os vários componentes em um ambiente 802.1X NAC quando o dispositivo tentando acessar a rede tem o agente LANDesk 802.1X instalado.

Configurar um servidor Radius 802.1X ou proxy

Conforme indicado anteriormente, o LANDesk 802.1X NAC melhora um ambiente NAC 802.1X existente adicionando funcionalidade de autenticação e conformidade. O LANDesk 802.1X NAC requer um servidor Radius 802.1X ou proxy Radius.

Escolha um dos seguintes métodos para implementar o LANDesk 802.1X NAC

- "Uso do plugin de servidor IAS Radius (para MD5)" na página 522
- "Uso do proxy Radius (para PEAP)" na página 525

NOTA: Use o plu-in de servidor Radius IAS se especificou EAP tipo MD5. Use o proxy Radius se especificar o EAP tipo PEAP. (Você pode usar também o proxy Radius se tiver um servidor Radius não-IAS.)

As seções abaixo fornecem instruções passo a passo para ambas as configurações.

IMPORTANTE: Configuração de switch e roteador
Após configura o servidor Radius é necessário também configurar o switch de rede e roteador para o LANDesk 802.1X NAC. O hardware do switch e do router são exclusivos a cada ambiente de rede, por isso não é possível fornecer instruções específicas para cada tipo de hardware aqui. Ao configurar o switch e roteador para 802.1X NAC, siga as diretrizes básicas para os requisitos de funcionalidade e topologia descritos no tópico "Fluxos de processo, topologia de rede e componentes 802.1X NAC" na página 519. Além disso, você pode ir para o site de suporte da LANDesk para ver as recomendação de configuração de switch e roteador e os arquivos de exemplo de configuração.

Uso do plugin de servidor IAS Radius (para MD5)

Use o plug-in de servidor 802.1X IAS para utilizar um servidor IAS existente (ou configurar um novo servidor IAS) para a autenticação do 802.1X.

As etapas abaixo descrevem como instalar (se necessário) e configurar um servidor IAS com o plug-in EAP. Conclua todas as etapas antes de habilitar o 802.1X no console.

Etapa 1: Instalar o servidor Radius e o tipo de LTA EAP

1. Instale o IAS (Internet Authentication Server) no servidor em que deseja configurar como o servidor Radius de acesso remoto. O IAS pode ser instalado do CD do Windows 2003. (**NOTA:** o protocolo Radius é aceito somente no Windows 2000 e no Windows 2003.) Siga os avisos de instalação.
2. Instale o tipo de LTA EAP no servidor Radius. O LTA EAP é o protocolo de autenticação proprietário. Instale-o do servidor núcleo. Mapeie uma unidade para o servidor núcleo e, em seguida, inicie o arquivo executável **LTAEAP.EXE** encontrado no diretório \LDMain\Install\Radius.
3. Reinicialize o servidor para registrar o LTA EAP no servidor.

NOTA: você pode verificar este novo tipo de EAP na página Propriedades do servidor remoto. Para fazer isso, vá para **Painel de controle > Ferramentas administrativas > Roteamento e acesso remoto**. Clique com o botão direito do mouse no servidor remoto, clique em **Propriedades**, clique na guia **Segurança**, clique em **Métodos de autenticação** e, finalmente, em **Métodos EAP**. O tipo de LTA EAP será exibido na lista de métodos. Caso contrário, ele deverá ser instalado do servidor núcleo.

Etapa 2: Configurar e iniciar o serviço de acesso remoto no servidor Radius

1. Clique em **Painel de controle > Ferramentas administrativas > Roteamento e acesso remoto**.
2. Clique com o botão direito do mouse no servidor e, em seguida, clique em **Configurar e habilitar roteamento e acesso remoto**. O Assistente para configuração do servidor de roteamento e acesso remoto é exibido.
3. Clique em **Avançar**.
4. Selecione **Configuração personalizada** e clique em **Avançar**.
5. Selecione **Acesso dial-up** e clique em **Avançar**.
6. Clique em **Concluir**.
7. Quando solicitado, clique em **Sim** para iniciar o serviço.

Etapa 3: Personalizar o serviço de acesso remoto (definir o EAP como o método de autenticação preferido para os dispositivos remotos)

1. Na ferramenta Roteamento e acesso remoto, clique com o botão direito do mouse no servidor que acabou de configurar e clique em **Propriedades**.
2. Na guia **Geral**, verifique se a opção **Servidor de acesso remoto** está marcada.
3. Na guia **Segurança**, marque a caixa de seleção **Extensible Authentication Protocol (EAP)**. (Talvez seja interessante clicar no botão **Métodos EAP** para ter certeza de que o novo método LTA EAP esteja na lista de métodos.)
4. Clique em **OK** para sair da caixa de diálogo Métodos de autenticação.
5. Clique em **OK** novamente para sair da caixa de diálogo Propriedades.

Criar uma diretiva de acesso remoto no servidor Radius

É necessário configurar uma diretiva de acesso remoto que use o método EAP para autenticação.

Você pode fazer isso nas ferramentas IAS ou Roteamento e acesso remoto.

Etapa 1: Criar a diretiva de acesso remoto

1. No nó do servidor de acesso remoto, clique com o botão direito do mouse em **Diretivas de acesso remoto** e, em seguida, clique em **Nova**. O assistente de diretivas de acesso remoto é exibido.
2. Clique em **Avançar**.
3. Selecione **Típica** como o tipo de diretiva, digite um nome para a diretiva e clique em **Avançar**. (Nota: Insira um nome descritivo que identifique facilmente a diretiva.)
4. Selecione **Ethernet** como o método de acesso e clique em **Avançar**.
5. Selecione **Usuário** para a concessão de acesso (e não Grupo) e, em seguida, clique em **Avançar**.
6. Selecione **LTA EAP** como o método de autenticação e, em seguida, clique em **Avançar**.
7. Clique em **Concluir** para criar a diretiva de acesso remoto.

Etapa 2: Configurar a diretiva de acesso remoto para oferecer suporte a redes com ou sem fio

1. Clique com o botão direito mouse na diretiva de acesso remoto que acabou de criar e, em seguida, clique em **Propriedades**.
2. Marque a opção **Conceder permissão de acesso remoto** para habilitar o suporte a redes sem fio.
3. Clique em **OK**.

Configurar (adicionar) switches de rede como clientes Radius

Agora é necessário adicionar os switches de rede (como clientes Radius) que serão usados com a autenticação do 802.1X.

Essa tarefa é executada na ferramenta IAS (**IAS > Clientes Radius**).

Quando um switch é adicionado como um cliente Radius, o servidor Radius é capaz de reconhecer e processar as solicitações de autenticação através do switch.

Criar um usuário comum no servidor Radius

Você agora deve criar um novo usuário no servidor Radius para estabelecer as credenciais de login. O nome e a senha deste usuário determinarão as credenciais de autenticação para os dispositivos gerenciados configurados com o NAC do 802.1X que tentam obter acesso à rede.

Use a ferramenta Gerenciamento do computador do servidor para executar esta tarefa.

Para criar um usuário no servidor Radius

1. No servidor Radius, clique em **Iniciar > Programas > Ferramentas administrativas > Gerenciamento do computador**.
2. Abra **Usuários e grupos locais**, clique com o botão direito do mouse em **Usuários** e, em seguida, clique em **Novo usuário**.
3. Digite um nome de usuário.
4. Digite uma senha e confirme-a.
5. Configure a senha com as seguintes opções:
    - Desmarque a caixa de seleção **O usuário deve alterar a senha no próximo logon**.
    - Marque a caixa de seleção **O usuário não pode alterar a senha**.
    - Marque a caixa de seleção **A senha nunca expira**.
    - Certifique-se de que a caixa de seleção **Conta desativada** esteja desmarcada.
6. Clique em **Criar**.

O nome de usuário e a senha fornecidos aqui são as credenciais de login que o usuário final deverá fornecer para responder com êxito à solicitação de identificação de autenticação durante o processo de autenticação do 802.1X. Em seguida, as credenciais serão enviadas para o servidor Radius, juntamente com os dados do EAP, para determinar se o dispositivo tem ou não permissão para acessar a rede.

Você pode também habilitar o 802.1X no console. (O outro método de implementar o 802.1X NAC é configurar e instalar um proxy Radius. Para obter mais informações, consulte "Uso do proxy Radius (para PEAP)" na página 525.

Habilitar o LANDesk 802.1X NAC com o plug-in do servidor Radius IAS

Após concluir todas as tarefas de configuração anotadas acima, você poderá habilitar a autenticação do 802.1X NAC.

Você faz isso do console (**Ferramentas > Segurança > Controle de acesso de rede**).

Essencialmente, os serviços de autenticação do 802.1X são ativados em sua rede. No entanto, você ainda deverá configurar os dispositivos gerenciados com o agente 802.1X para que seus acessos à rede possam ser gerenciados e controlados pela autenticação do 802.1X. Para obter mais informações, consulte "Distribua o agente LANDesk 802.1x NAC para os dispositivos gerenciados" na página 528.

Para habilitar o LANDesk 802.1X NAC com o plug-in do servidor Radius IAS

1. Na ferramenta de **Controle de acesso de rede**, clique com o botão direito em **802.1X** e clique em **Configurar 802.1X > Servidor Radius**.

2. Marque a caixa de seleção **Habilitar o servidor Radius 802.1X**. A autenticação do 802.1X é ativada em sua rede (para os dispositivos com o agente 802.1X) usando o servidor Radius IAS com o plug-in EAP que você configurou.
3. Para o **Tipo de EAP**, selecione MD5.
4. Selecione **Utilizar o plug-in IAS do LTA EAP**.
5. Clique em **Salvar**.

A seção a seguir descreve como configurar o 802.1X NAC usando o método de proxy Radius.

Uso do proxy Radius (para PEAP)

Uso do proxy Radius se quiser utilizar o EAP tipo PEAP. (Você pode usar também o proxy Radius se tiver um servidor Radius não-IAS.)

O proxy Radius 802.1X pode ser instalado nos seguintes tipos de servidores Radius:

- Cisco ACS
- A10 Networks
- CAMS (Comprehensive Access Management System)
- IAS (Internet Authentication Service)

IMPORTANTE: Coexistência com o software do servidor Radius
O proxy Radius do 802.1X pode coexistir em servidores que executam o software de servidor Radius. Se o seu servidor Radius for um servidor baseado em hardware, instale o proxy Radius 802.1X em um servidor separado.

O proxy Radius faz a comunicação entre o switch e o dispositivo com o agente 802.1X instalado. O proxy situa-se no meio: o dispositivo é autenticado no proxy Radius, o qual transmite o ID e a senha para o servidor Radius. Se o agente não estiver instalado no dispositivo que tentou fazer a conexão, o proxy Radius negará o acesso.

Habilitar o LANDesk 802.1X NAC com o proxy Radius

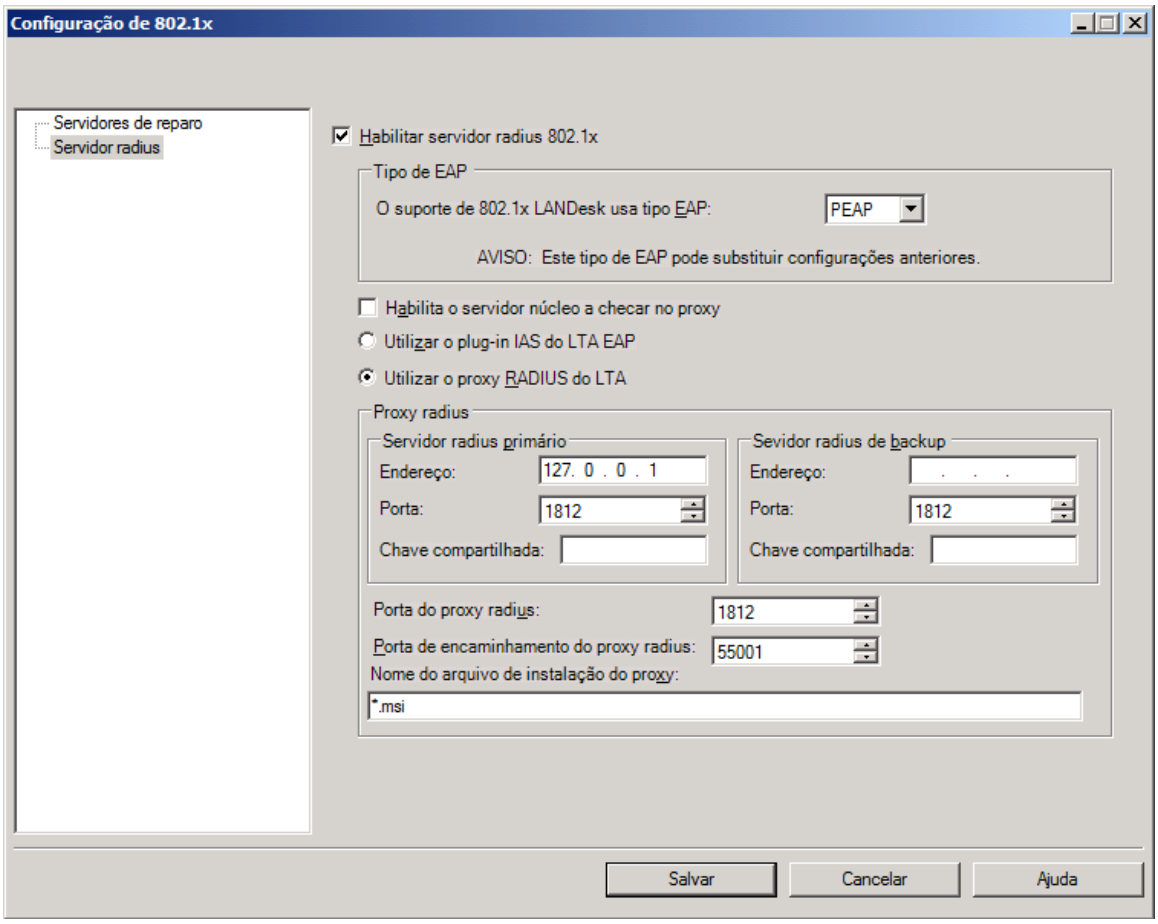
Para usar o proxy Radius é preciso habilitar o LANDesk 802.1X NAC, configurar os parâmetros para um arquivo de instalação de proxy Radius e instalar o proxy Radius no seu servidor Radius.

Você faz isso do console (**Ferramentas > Segurança > Controle de acesso de rede**).

Isto basicamente ativa os serviços de autenticação do 802.1X em sua rede. No entanto, você ainda deverá configurar os dispositivos gerenciados com o agente 802.1X para que seus acessos à rede possam ser gerenciados e controlados pela autenticação do 802.1X. Para obter mais informações, consulte "Distribua o agente LANDesk 802.1x NAC para os dispositivos gerenciados" na página 528.

Para habilitar o LANDesk 802.1X NAC e configurar um arquivo de instalação de proxy Radius

1. Na janela da ferramenta de **Controle de acesso de rede**, clique com o botão direito no objeto **802.1X** e clique em **Configurar 802.1X** e em seguida, clique em **Servidor Radius**.



2. Marque a caixa de seleção **Habilitar o servidor Radius 802.1X**. O processo de autenticação do 802.1X em sua rede (para os dispositivos com o agente 802.1X) é ativado após a instalação do proxy Radius que está sendo configurado aqui.
3. Para o **Tipo de EAP**, selecione PEAP.
4. Se você quiser verificar o servidor núcleo, selecione a caixa de seleção **Ativar a verificação do servidor núcleo no proxy**.
5. Selecione **Usar proxy Radius LTA**.
6. Digite as informação para um servidor Radius primário. (Se quiser usar um servidor Radius de backup, digite as informações para um sevidor secundário também.)
7. Digite um nome para o arquivo de instalação (MSI) do proxy Radius. O arquivo de instalação é criado no diretório LDMAIN\Install\Radius. É possível ter vários arquivos de instalação de servidor proxy Radius. (**NOTA:** O proxy Radius funciona em qualquer plataforma Windows de 32 bits.
8. Clique em **Salvar**.

Para instalar um proxy Radius

1. No servidor que você deseja configurar com o proxy Radius 802.1X, conecte-se ao servidor núcleo e vá para a pasta em que você salvou o arquivo de instalação do proxy.

2. Clique duas vezes no arquivo MSI para executar a instalação.
3. Clique em **Fechar** quando a instalação estiver concluída. Não é necessário reinicializar o sistema.

A instalação do proxy Radius adiciona dados (como endereço e informações de porta) ao Registro do servidor.

AVISO: Não há suporte para plataformas de 64 bits
Não instale o proxy Radius no Windows 98 ou em nenhuma plataforma de 64 bits.

A seção a seguir descreve as caixas de diálogo mencionadas nas tarefas acima.

Ajuda do servidor e do 802.1X

Sobre a caixa de diálogo Definições de configuração do 802.1X:

Use essa caixa de diálogo para selecionar um servidor de correção e publicar as configurações de controle de acesso à rede para ele e para ativar o 802.1X NAC na rede.

Se você estiver usando o plug-in de servidor Radius IAS, basta ativar o servidor Radius e especificar o tipo de EAP e selecionar a opção de plug-in IAS.

Se estiver usando o proxy Radius, é preciso não só habilitar o servidor Radius e especificar o tipo EAP (PEAP), mas é necessário também configurar um arquivos de instalação do proxy Radius e, em seguida, instalar o proxy Radius no seu servidor designado.

Essa caixa de diálogo contém duas páginas:

Sobre a página Servidores de correção

- **Adicionar:** Abre o diálogo onde você pode especificar o servidor de correção que deseja usar para corrigir os dispositivos com mal funcionamento alocados na rede de quarentena. Clique em **Ajudar** para obter informações sobre o servidor de correção. Um servidor de correção contém os arquivos de configuração e suporte necessários (cliente de segurança, definições de tipo de segurança e patches solicitados), bem como as páginas modelo HTML usadas para analisar os dispositivos em busca de vulnerabilidades identificadas pela diretiva de segurança. Com esses recursos, o servidor de recuperação repara todas as vulnerabilidades para que o dispositivo possa ser analisado como em funcionamento (ou compatível) e acessar a rede.
- **Remover:** Exclui o servidor de correção selecionado.
- **Modificar:** Permite editar o servidor de correção selecionado.
- **Publicar:** Abre um diálogo onde você pode publicar configurações NAC para validação de postura e servidores de correção.

Sobre a página Servidor Radius

- **Habilitar o servidor Radius 802.1X:** Ativa o suporte LANDesk 802.1X NAC (autenticação e conformidade).

  NOTA: Por padrão, esta opção não é selecionada, o que basicamente permite o acesso à rede para todos os dispositivos que tentam se conectar, sejam eles confiáveis ou não. Mantenha esta opção desmarcada para permitir o acesso de todos à rede.

- **Tipo de EAP:** identifica o tipo de EAP usado pela autenticação do 802.1X. Selecione PEAP para uma implementação de proxy de Radius. Selecione MD5 para uma implementação de plug-in de servidor Radius IAS.
- **Utilizar o plug-in IAS do LTA EAP:** Selecione esta opção quiser usar um servidor IAS existente.
- **Utilizar proxy Radius LTA:** Selecione esta opção se quiser utilizar o EAP tipo PEAP. Com esta opção selecionada, você pode configurar um arquivo de instalação de proxy Radius 802.1X.
- **Proxy Radius:** Digite as informação para um servidor Radius primário. (Se quiser usar um servidor Radius de backup, digite as informações para um sevidor secundário também.)
    - **Endereço do servidor Radius:** especifica o endereço IP do servidor Radius.
    - **Porta do servidor Radius:** especifica o número da porta do servidor Radius. O número da porta padrão para a autenticação do Radius é a porta de UDP 1812.
    - **Chave compartilhada:** Especifica a chave compartilhada (ou o segredo compartilhado) que proporciona a segurança da comunicação entre o switch e o servidor Radius. A chave compartilhada é uma seqüência de caracteres de texto. A string inserida aqui precisa corresponder à string da chave compartilhada configurada no switch e no servidor Radius.
- **Porta do proxy Radius:** especifica o número da porta do proxy Radius. A comunicação com o switch é feita por meio desta porta. Observe que este número deverá ser diferente da porta do servidor Radius (acima) se ambas estiverem na mesma máquina.
- **Porta de porta de encaminhamento do proxy:** especifica o número da porta de encaminhamento do proxy Radius. Essa porta é usada no encaminhamento dos dados para o servidor Radius.
- **Nome do arquivo de instalação do proxy:** identifica o arquivo de instalação do proxy Radius. O arquivo de instalação é criado no diretório LDMain, em Install\Radius\. É possível criar vários arquivos de instalação do proxy Radius. O proxy Radius funciona em qualquer plataforma Windows de 32 bits.

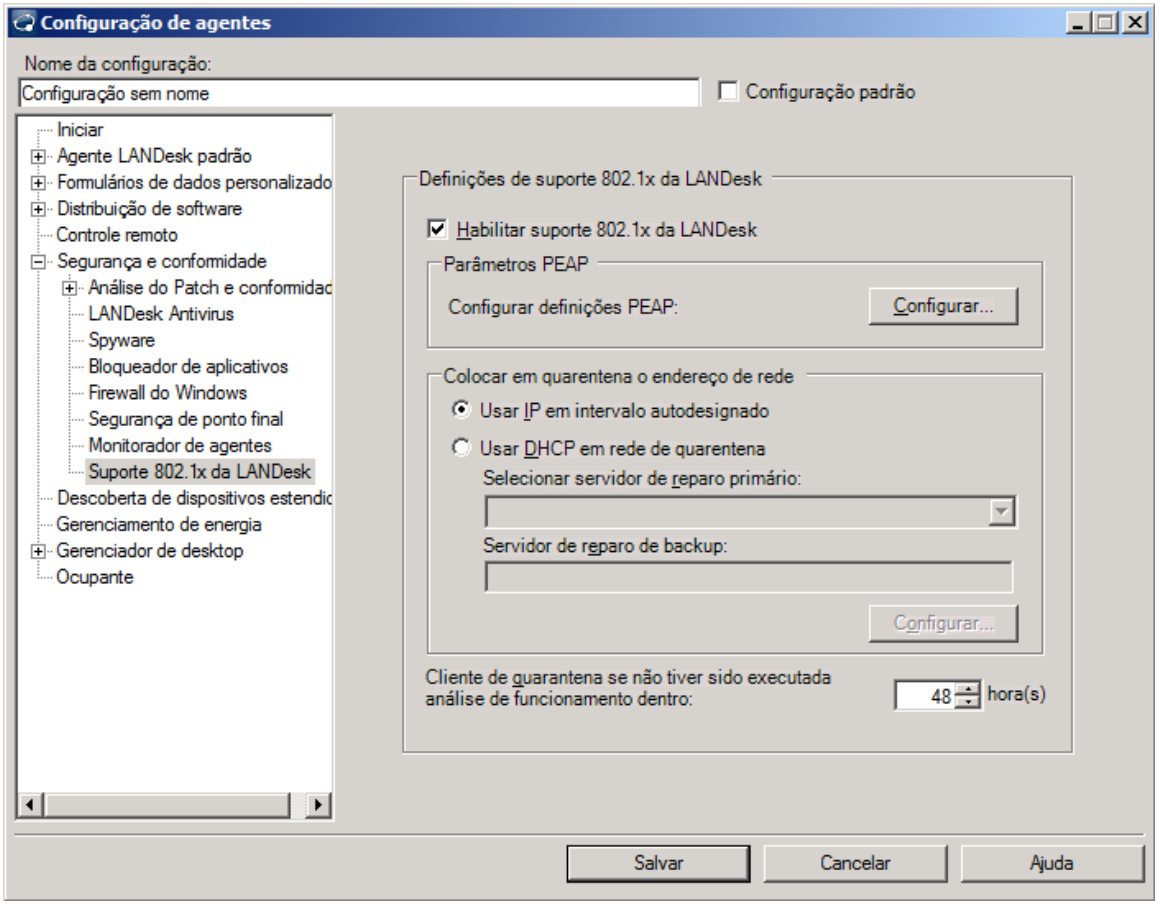
Distribua o agente LANDesk 802.1x NAC para os dispositivos gerenciados

A etapa final da configuração do suporte ao LANDesk 802.1X é a distribuição do agente 802.1X para os dispositivos alvo gerenciados.

Isso habilita a análise de conformidade e permite aos dispositivos gerenciados serem autenticados e receberem permissão de acesso à rede ou serem colocados em quarentena e corrigidos.

Para distribuir o agente 802.1x para os dispositivos gerenciados

1. Na ferramenta **Configuração do agente**, clique em **Nova configuração do Windows**, abra o nó **Segurança e conformidade** e, a seguir clique em **Suporte ao LANDesk 802.1X**.

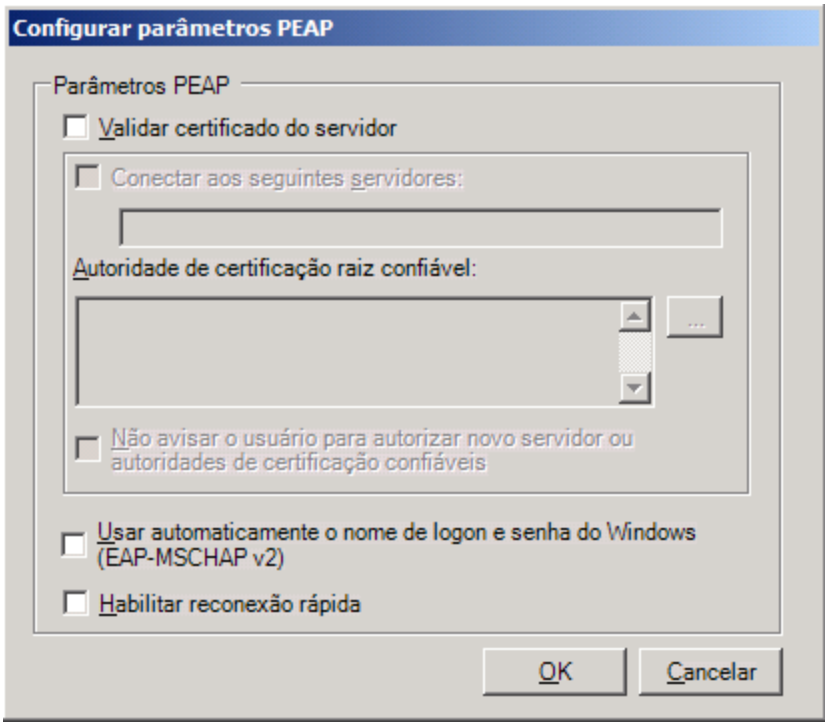


2. Marque a caixa de seleção **Habilitar o suporte para LANDesk 802.1X**.

   IMPORTANTE: Esta opção não estará disponível se o Servidor Radius 802.1X já não tiver sido configurado na ferramenta NAC do console.

   NOTA: O 802.1X NAC usa o tipo EAP especificado na ferramenta NAC (PEAP ou MD5). A opção de tipo de EAP é válida no núcleo inteiro. Em outras palavras, todos os dispositivos com esta configuração de agente serão definidos com o tipo de EAP especificado no console.

3. Se estiver usando o EAP tipo PEAP, clique em **Configurar**.


Configurar parâmetros PEAP
Parâmetros PEAP
Validar certificado do servidor
Conectar aos seguintes servidores:
Autoridade de certificação raiz confiável:
...
Não avisar o usuário para autorizar novo servidor ou autoridades de certificação confiáveis
Usar automaticamente o nome de logon e senha do Windows (EAP-MSCHAP v2)
Habilitar reconexão rápida
OK
Cancelar

4. Especifique as seguintes configurações PEAP e clique em **OK**.
   - **Validar certificado de servidor:** Indica que pode-se confirar no arquivo de certificado do servidor Radius.
   - **Conecatr a estes servidores:** Fornece outra verificação de validação ao deixar você identificar servidores específicos nos quais pode confiar. Digite os nomes de servidor (nomes DNS completamente qualificados) separados por espaços.
   - **Autoridade de certificação de raiz confiável:** Importa o arquivo do certificado confiável.
   - **Não avisar o usuário para autorizar novo servidor:** Desativa o aviso de autorização nos dispositivos dos usuários finais.
   - **Usa automaticamente o nome e a senha de logon do Windows:** Usa as credenciais de logon do Windows para que elas não precisem ser digitadas mais de uma vez.
   - **Habilitar reconexão rápida:** Faz o cache das credenciais de logon para um login rápido se o tempo limite do dispositivo expirar.
5. Na caixa de diálogo Configuração do agente, selecione o método que deseja usar para colocar em quarentena quaisquer dispositivos em mal funcionamento encontrados. (Use endereço IP em um intervalo auto-atribuído ou use o DHCP na rede em quarentena.)
6. Configure o tempo de quarentena automática especificando quantas horas podem ocorrer desde a última análise de conformidade em um dispositivo antes que ele seja considerado sem conformidade e desconectado da rede corporativa e colocado em rede de quarentena.
7. Especifique qualquer outra opção de configuração de agente de dispositivo que deseje aplicar ao dispositivo que está sendo configurado.
8. Clique em **Salvar**.

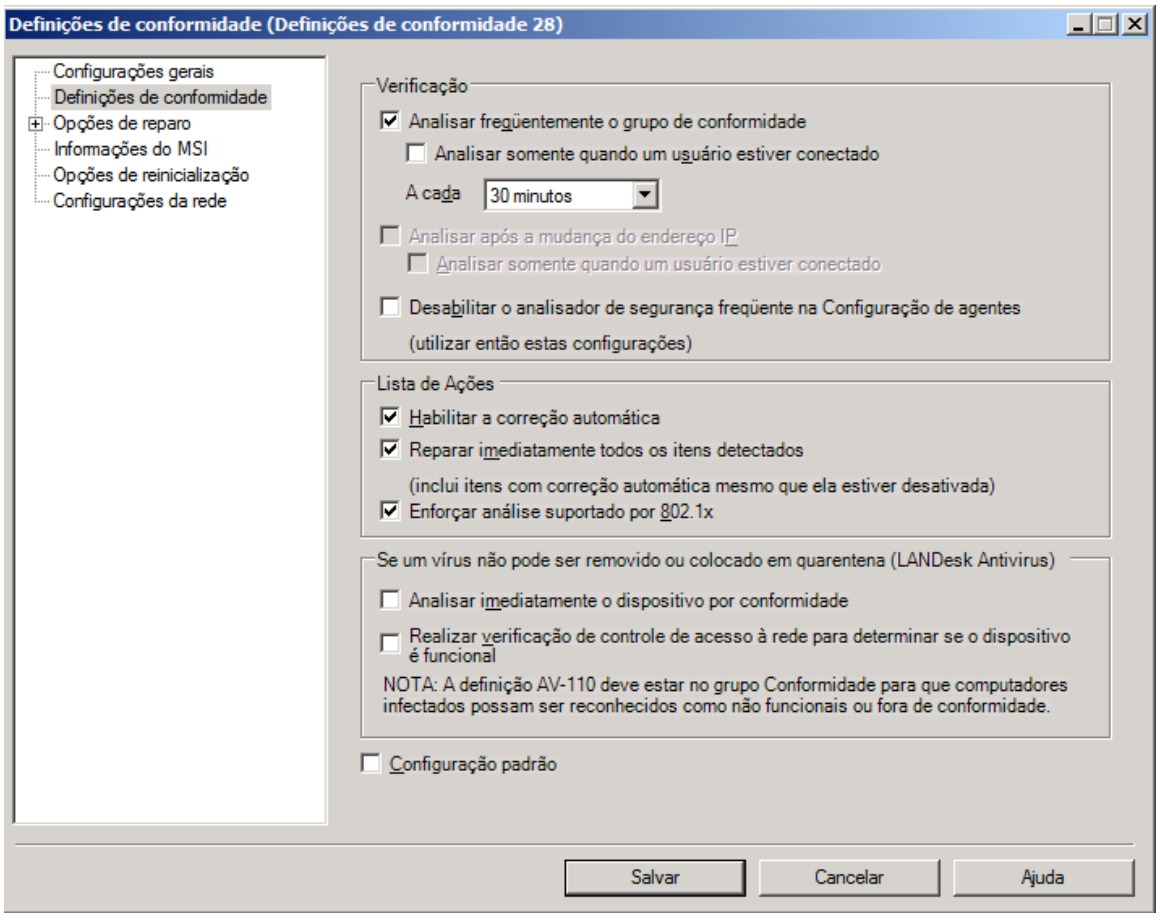
Agora você pode distribuir a configuração do agente para os dispositivos alvo onde deseja usar LANDesk 802.1X NAC e depois pode criar tarefas de análise de conformidade que analisem dispositivos com o 802.1X ativado para conformidade com sua diretiva de segurança.

Criar tarefas de análise de segurança de conformidade

O Controle de acesso de rede executa então uma análise de segurança de conformidade que determina a postura ou o status de funcionamento do dispositivo de acordo com o critério definido pela sua diretiva de segurança de conformidade.

Uso das configurações de conformidade

A análise de conformidade é executada por uma tarefa de análise de conformidade, usando as configurações de conformidade com a opção **Impor a análise de 802.1X suportada** ativada na página **Conformidade**.


Definições de conformidade (Definições de conformidade 28)
Configurações gerais
Definições de conformidade
Opções de reparo
Informações do MSI
Opções de reinicialização
Configurações da rede
Verificação
Analisar freqüentemente o grupo de conformidade
Analisar somente quando um usuário estiver conectado
A cada
30 minutos
Analisar após a mudança do endereço IP
Analisar somente quando um usuário estiver conectado
Desabilitar o analisador de segurança freqüente na Configuração de agentes
(utilizar então estas configurações)
Lista de Ações
Habilitar a correção automática
Reparar imediatamente todos os itens detectados
(inclui itens com correção automática mesmo que ela estiver desativada)
Enforçar análise suportado por 802.1x
Se um vírus não pode ser removido ou colocado em quarentena (LANDesk Antivirus)
Analisar imediatamente o dispositivo por conformidade
Realizar verificação de controle de acesso à rede para determinar se o dispositivo é funcional
NOTA: A definição AV-110 deve estar no grupo Conformidade para que computadores infectados possam ser reconhecidos como não funcionais ou fora de conformidade.
Configuração padrão
Salvar
Cancelar
Ajuda

Use a ferramenta Patch e conformidade (**Ferramentas > Segurança > Patch e conformidade**) para criar análises de segurança de conformidade. Para ver as instruções passo a passo, veja "Criar tarefas de análise de segurança e conformidade" na página 591.

NOTA: Análises de segurança de conformidade
Com a ferramenta Patch e conformidade Manager, você pode criar e configurar uma análise de segurança específica de conformidade, que verifica a conformidade dos dispositivos alvo com a sua diretiva de

segurança personalizada. Uma análise de conformidade é baseada no conteúdo do grupo Conformidade e pode ser executada como uma tarefa agendada ou uma diretiva. Para informações sobre a atualização de diretivas e regras de segurança de conformidade e sobre a republicação de parâmetros do NAC, consulte "Primeiro, verifique se o suporte ao 802.1X NAC está habilitado" na página 544.

Configurar um switch e roteador para suporte para LANDesk 802.1X NAC

O LANDesk 802.1X NAC requer um switch e roteador para executar autenticação e conformidade.

O hardware do switch e roteador são exclusivos a cada ambiente de rede, por isso não é prático fornecer instruções específicas para cada tipo de hardware aqui. Entretanto, como diretriz geral quando configurar o seu switch e roteador para o LANDesk 802.1X NAC, verifique se eles satisfazem os requisitos de funcionalidade e topologia descritos naquelas seções acima. Para obter mais informações, consulte "Fluxos de processo, topologia de rede e componentes 802.1X NAC" na página 519

Além disso, você pode ir para o site de suporte da LANDesk para ver as recomendação de configuração de switch e roteador e os arquivos de exemplo de configuração.

NOTA: A Comunidade de usuários da LANDesk
A Comunidade de usuários LANDesk tem fóruns de usuários e os melhores métodos conhecidos para todos os produtos e tecnologia da LANDesk. Para acessar esse recurso valioso, visite: http://community.landesk.com

Instalar e configurar um servidor de correção

O Network Access Control (NAC) requer um servidor de correção para reparar dispositivos vulneráveis ou infectados. O servidor de correção é onde um dispositivo, cuja postura foi determinada como sendo em estado de não funcionamento, é enviado para ser corrigido (reparado) de forma a satisfazer as regras de conformidade configuradas para um status de funcionamento.

O servidor de correção é onde são publicados os recursos de correção como, clientes de segurança que buscam por vulnerabilidades e outros riscos de segurança nos dispositivos, arquivos patch e páginas HTML que aparecem nos dispositivos e fornecem opções para correção ou acesso limitado à rede.

Pré-requisitos do servidor de correção

O computador que você deseja configurar como servidor de correção deve satisfazer os seguintes requisitos:

- O servidor de correção pode ser qualquer tipo de servidor Web, tal como o IIS do Windows, ou Apache no Linux
- É necessário criar um compartilhamento de web no servidor de correção que tem acesso anônimo com direitos de leitura e de procurar (navegação) ativados. Para obter instruções detalhadas, consulte "Criar um compartilhamento Web no servidor de correção" na página 533.

IMPORTANTE: Criação de um compartilhamento do Samba
Se estiver usando um servidor de web Apache em Linux, o compartilhamento que criar será Samba.

Determinar o local do servidor de correção na rede

Ao decidir o local do servidor de correção na rede Cisco é necessário satisfazer as seguintes diretrizes.

- O próprio servidor de correção pode ser colocado em qualquer lado do roteador.
- Se decidir colocá-lo no lado do cliente do roteador, ele estará mais seguro porque não é necessário fazer nenhuma exceção às regras do roteador, mas você terá que passar todos os arquivos de correção manualmente para o computador cada vez que mudá-los.
- Se os colocar no lado oposto do roteador, haverá risco potencial de segurança, pois os computadores de quarentena estarão acessando um computador na rede, entretanto você pode enviar os arquivos de correção para o computador sem precisar levá-los manualmente.
- O servidor de correção deve estar visível na VLAN de correção.
- Você pode ter mais de um servidor de correção em sua rede.

Você pode encontrar diagramas que mostram o local do componente e o fluxo de trabalho do processo do LANDesk 802.1X NAC na seção de visão geral.

Criar um compartilhamento Web no servidor de correção

O procedimento de criação e configuração de um compartilhamento da Web no servidor de correção foi automatizado por um script localizado no servidor núcleo que você pode executar a partir do computador que você quer configurar como um servidor de correção.

O compartilhamento de Web que é criado no servidor de correção funciona como uma área de armazenamento para os arquivos patch executáveis que são usados para corrigir vulnerabilidades em dispositivos afetados. Quando você publica arquivos de infra-estrutura ou recursos de correção (por exemplo, cliente de segurança, arquivos patch e arquivos HTML) do servidor núcleo, esses arquivos são copiados nesse compartilhamento de Web.

IMPORTANTE: O compartilhamento de web deve ser denominado LDLogon.
O nome do compartilhamento de Web deve ser LDLogon. Você pode criar esse compartilhamento em qualquer lugar no servidor de Web. O caminho típico de um compartilhamento seria: C:\Inetpub\wwwroot\LDLogon. Mas o compartilhamento pode ser criado em qualquer caminho desde que a redireção do URL seja configurada para: http://servername/LDLogon.

Após executar o script para criar e configurar o compartilhamento Web, é necessário adicionar o servidor de correção no console e especificar o caminho para o compartilhamento (para obter instruções detalhadas, consulte "Configurar (adicionar) um servidor de correção no console" na página 534). Isso garante que o servidor núcleo publique recursos de correção para o local correto no servidor de correção.

Para executar o script de configuração do servidor de correção

1. No computador que quiser configurar como servidor de correção, mapeie uma unidade à pasta LDMain\Install\TrustedAccess\RemediationServer do servidor núcleo.
2. Clique duas vezes no script de configuração CONFIGURE.REMEDIATION.SERVER.VBS.

Servidor de correção configurado automaticamente

O script de configuração do servidor de correção configura automaticamente o servidor para executar a correção, fazendo o seguinte:

- Criando um compartilhamento de Web chamado LDLogon em: c:\inetpub\wwwroot\LDLogon
- Habilitando o acesso anônimo ao compartilhamento LDLogon com direitos de Leitura, Gravação e Procura.

- Adicionando um novo tipo de MIME para os arquivos .lrd e definindo-o para aplicativo/octeto-fluxo (aplicativo/binário).

NOTA: Use também a ferramenta Microsoft IIS para configurar manualmente as permissões de acesso do compartilhamento LDLogon e os tipos de MIME.

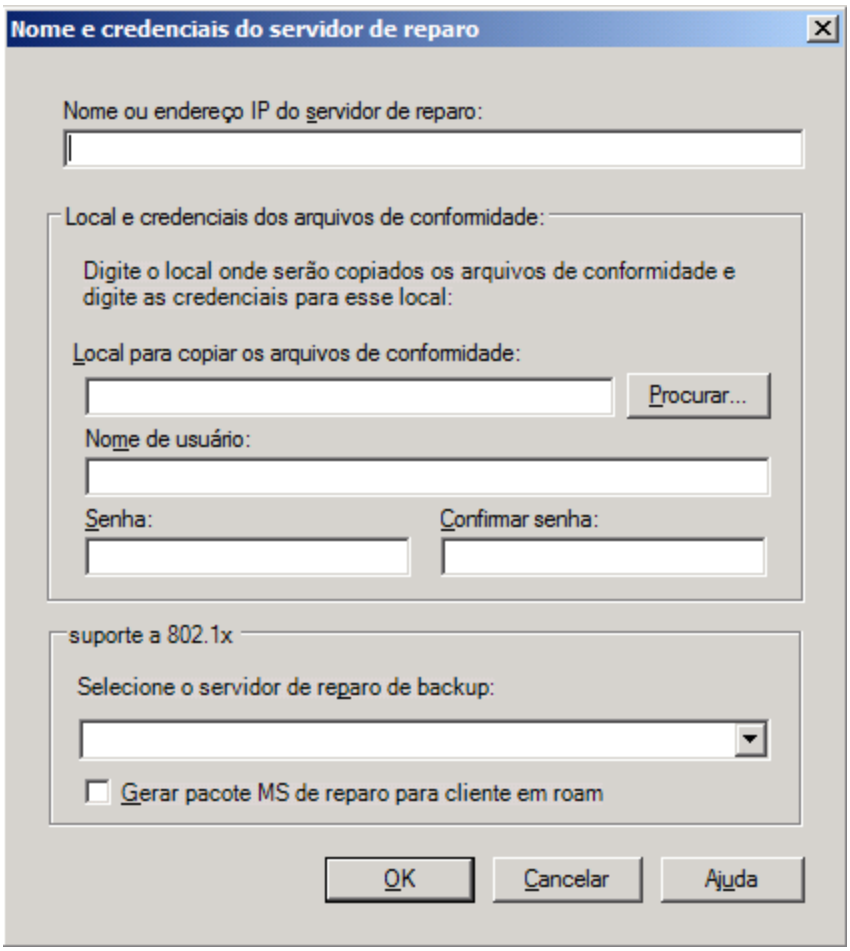
O servidor de correção está agora pronto para ser configurado (p. ex., adicionado) no console.

Configurar (adicionar) um servidor de correção no console

Com o servidor de correção configurado, é necessário configurá-lo e adicioná-lo à lista de servidores de correção válidos na caixa de diálogo **Configurar servidores de correção** no console. Ao fazer isso, o servidor de correção é reconhecido na rede e poderá comunicar-se corretamente com os outros componentes NAC.

Para configurar e adicionar servidores de correção no console

1. Na ferramenta de **Controle de acesso de rede**, clique com o botão direito em **802.1X** e clique em **Configurar 802.1X**.
2. Na página **Servidores de correção**, clique em **Adicionar**. A caixa de diálogo **Nome e credenciais do servidor de correção** é exibida.


Nome e credenciais do servidor de reparo
Nome ou endereço IP do servidor de reparo:
Local e credenciais dos arquivos de conformidade:
Digite o local onde serão copiados os arquivos de conformidade e digite as credenciais para esse local:
Local para copiar os arquivos de conformidade:
Procurar...
Nome de usuário:
Senha:
Confirmar senha:
suporte a 802.1x
Selecione o servidor de reparo de backup:
Gerar pacote MS de reparo para cliente em roam
OK
Cancelar
Ajuda

3. Digite o nome do servidor e o endereço IP do servidor de correção.
4. Digite o caminho do compartilhamento de web (no servidor de web que estiver configurando como servidor de correção) onde quer publicar os arquivos de conformidade. O compartilhamento de web deve ser denominado LDLogon. Os arquivos de conformidade são os arquivos de definições de segurança que definem a sua diretiva de segurança de conformidade (ou seja, o conteúdo do grupo **Conformidade** em Patch e conformidade, assim como os arquivos de patch requeridos que corrigem as vulnerabilidades detectadas).

   Digite um caminho UNC ou um caminho de unidade mapeada. O caminho UNC é o método mais confiável porque as unidades mapeadas podem mudar (veja adiante). Clique no botão Procurar para navegar para o compartilhamento onde quer publicar arquivos de conformidade no servidor de correção.

   Importante: Se digitar um caminho local ou uma unidade mapeada no campo **Local para a cópia de aquivos de conformidade** os arquivos serão publicados no computador local ou na unidade mapeada especificada no computador onde a publicação for iniciada. Para assegurar que os arquivos de conformidade sejam publicados no mesmo local em cada servidor de correção na rede, recomendamos utilizar um caminho UNC para um compartilhamento de rede.

5. Digite um nome de usuário e uma senha válidos para acessar o servidor de correção.
6. Se você configurou mais de um servidor de correção, você pode selecionar um servidor de correção na lista suspensa.
7. Se quiser poder configurar um servidor de correção em outra rede, para dispositivos que são mudados entre redes confiáveis, gere um pacote de instalação (MSI).
8. Clique em **OK** para adicionar o servidor de correção à lista.

Agora é possível publicar os arquivos de infra-estrutura de correção no servidor (desde que tenha configurado também um servidor de validação de postura e as credenciais de usuário).

Sobre a caixa de diálogo Nome e credenciais do servidor de correção

Use esta caixa de diálogo para identificar o servidor de correção e o caminho para o compartilhamento de Web no servidor de correção onde os recursos de correção (clientes de segurança, arquivos patch e páginas HTML) são publicados.

- **Nome ou endereço IP do servidor de correção :** identifica o servidor de correção pelo seu endereço IP ou nome de host.
- **Local para copiar os arquivos de conformidade:** Especifique o caminho completo para o compartilhamento de web localizado no servidor de correção onde os arquivos de conformidade são publicados do núcleo. O nome do compartilhamento de web deve ser LDLogon. O caminho pode ser UNC ou uma unidade mapeada (ou caminho local). É recomendado um caminho UNC (veja a nota **Importante** acima).
- **Procurar:** Abre a janela local do Windows Explorer onde você pode navegar para o compartilhamento LDLOGON do servidor de correção.
- **Nome de usuário:** identifica um usuário válido com credenciais de acesso para o compartilhamento de web no servidor de correção.
- **Senha:** Identifica a senha do usuário.
- **Confirmar senha:** Verifica a senha do usuário.

- **OK:** salva as configurações do servidor de correção e o adiciona à lista no diálogo Configurar servidores de correção.
- **Selecionar backup do servidor de correção:** Se você configurou mais de um servidor de correção, você pode selecionar um servidor de correção na lista suspensa.
- **Gerar pacote de MSI de correção para cliente em roam:** Use esta opção para criar um pacote de instalação (MSI) que você pode usar para configurar um servidor de correção em outra rede para dispositivos portáveis que se mudam para outras redes.
- **Cancelar:** Fecha a caixa de diálogo sem salvar as configurações e sem adicioná-la à lista de servidores de correção.

Publicar arquivos de infra-estrutura de correção para servidores de correção

A etapa seguinte na instalação e configuração de um servidor de correção é a publicação no servidor de correção dos recursos vitais de infra-estrutura de correção do servidor núcleo. Esses recursos de infra-estrutura de correção são:

- Cliente de segurança (utilitário de análise de vulnerabilidade)
- Patches associados com as vulnerabilidade contidas no grupo Conformidade
- As páginas HTML que fornecem vínculos permitindo que usuários finais instalem agentes de confiáveis, executar análises de conformidade de segurança e corrigir vulnerabilidades detectadas e outras exposições de segurança.

Para poder fazer as publicações nos servidores é necessário, antes, definir seus critérios de segurança de conformidade na ferramenta Patch e conformidade.

Para obter mais informações, consulte "Definir critérios de segurança de conformidade na ferramenta Patch e conformidade" na página 536.

Definir critérios de segurança de conformidade na ferramenta Patch e conformidade

Após ter configurado o suporte a LANDesk 802.1X NAC no seu ambiente, você pode executar estas tarefas de gerenciamento de segurança de conformidade.

NOTA: Servidores adicionais necessários para o LANDesk 802.1X NAC
Para Controle de acesso à rede um servidor de correção já deve ter sido definido e configurado (ou adicionado) ao console. Para 802.1X NAC, você precisa também ter um servidor Radius 802.1X. Para obter mais informações, respectivamente, consulte "Instalar e configurar um servidor de correção" na página 532 e "Visão geral da ferramenta LANDesk 802.1X NAC" na página 517.

Outras tarefas de gerenciamento de segurança de conformidade

Para saber mais sobre a análise de conformidade e outras tarefas de gerenciamento do NAC como atualização das regras e diretivas de segurança de conformidade nos servidores de postura, atualização de recursos de correção nos servidores de correção, adição de dispositivos não gerenciados à ferramenta Descoberta de dispositivo não gerenciado, exame de dispositivos afetados, configuração de login e geração de relatórios, consulte "Primeiro, verifique se o suporte ao 802.1X NAC está habilitado" na página 544.

Define critérios de segurança de conformidade

Os critérios de segurança de conformidade são definidos pelos seguintes fatores:

- Conteúdo de segurança no **Grupo de conformidade** na ferramenta Patch e conformidade.
- A **configuração de tempo de quarentena automática** especificada na página **Suporte ao LANDesk 802.1X** na configuração de agente.

Consulte abaixo os procedimentos adequados para cada uma dessas tarefas. Consulte "Visão geral da ferramenta LANDesk 802.1X NAC" na página 517.

Sobre as assinaturas de conteúdo do Security Suite

É necessário ter uma assinatura de conteúdo do LANDesk Security Suite para o download dos vários tipos de conteúdo de segurança, tais quais definições de vulnerabilidade de aplicativo e sistemas operacionais (e patches requeridos), definições de spyware, definições de aplicativos bloqueados, definições de vírus, definições de ameaça de segurança a configuração de sistema e assim por diante.

Sem uma licença de Security Suite você não pode acessar os Serviços de segurança e não pode definir segurança de conformidade usando essas definições de segurança.

Download de definições dos tipos de segurança

Use a ferramenta Patch e conformidade para descarregar diferentes definições de tipos de segurança como definições de vulnerabilidade, spyware, antivírus e ameaça à segurança. Para obter mais informações sobre o uso dos recursos de download de Patch e conformidade, consulte "Download das atualizações do conteúdo de segurança" na página 571.

Usar o grupo Conformidade para definir uma diretiva de segurança de conformidade

Conforme explicado anteriormente, o conteúdo do grupo Conformidade determina a sua base de diretiva de segurança de conformidade. É possível configurar uma segurança de conformidade mínima composta apenas de algumas definições de vulnerabilidade e de ameaças à segurança ou, você pode criar uma diretiva de segurança complexa e estrita composta de várias definições de segurança. Você pode, também, modificar a diretiva de segurança de conformidade a qualquer momento adicionando e removendo definições do grupo Conformidade.

NOTA: Direito de Pach e Conformidade necessário
Somente um administrador ou um usuário com direito de Patch e conformidade pode adicionar ou remover definições do grupo Conformidade.

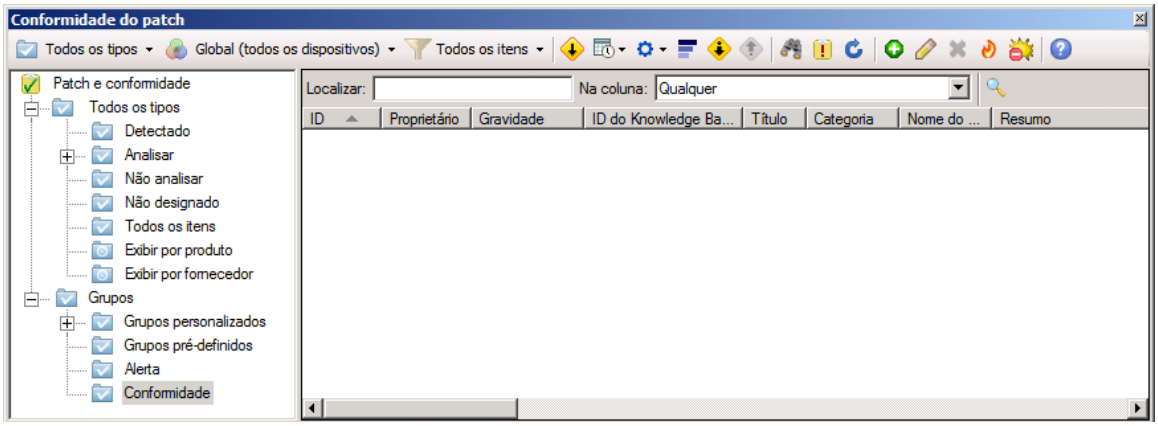
Os seguintes tipos de conteúdo de segurança podem ser adicionados ao grupo Conformidade para definir a conformidade dessa diretiva:

- Definições de antivírus
- Definições personalizadas
- Definições de atualização de driver
- Definições de atualização de software LANDesk
- Definições de ameaça de segurança (inclui definições de firewall)
- Definições de atualização de software
- Definições de spyware
- Vulnerabilidades (definições de vulnerabilidade de SO e aplicativo)

NOTA: Não é possível adicionar definições de aplicativo ao grupo Conformidade para definir diretivas de conformidade:

Para adicionar definições de segurança ao grupo Conformidade

1. Na ferramenta **Patch e conformidade**, selecione o tio de conteúdo de segurança que deseja adicionar à diretiva de segurança da lista suspensa **Tipo** e a seguida arraste e solte as definições da lista no grupo **Conformidade**.



2. Ou, clique com o botão direito em uma definição individual ou grupo selecionado de definições e clique em **Adicione o grupo conformidade**.
3. Certifique-se que as correções associadas necessárias foram descarregadas antes da publicação do conteúdo do NAC para os servidores de validação de postura e servidores de correção. Clique com o botão direito em uma definição, em grupos de definições ou no próprio grupo **Conformidade**, e clique em **Download de patches associados** para descarregar os patches necessários para corrigir os dispositivos afetados.

Publicar as configurações de NAC em servidores

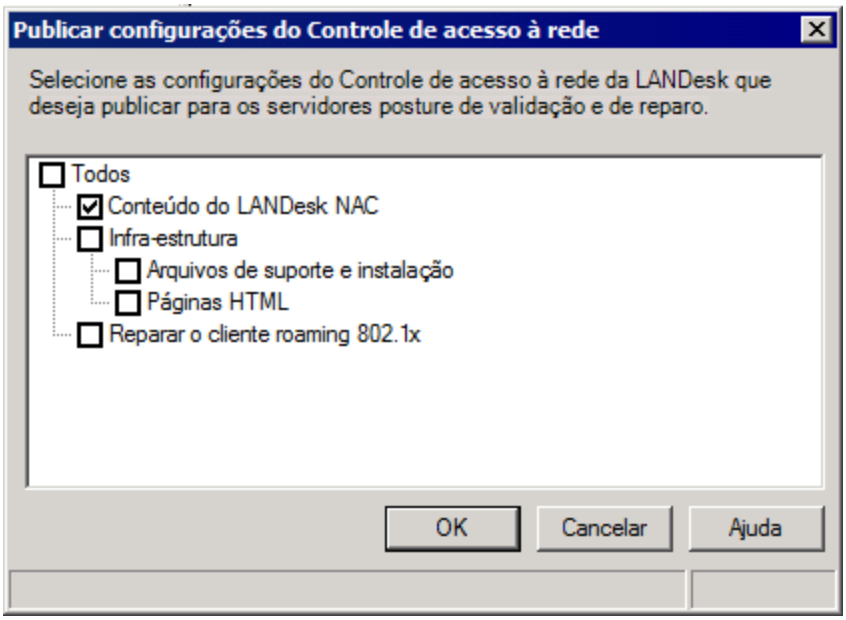
A publicação de parâmetros do NAC envia informações e recursos para os servidores de validação de postura e servidores de correção que são requeridas para a implementação do processo de validação de postura e fazer cumprir a diretiva de conformidade.

Para publicar as configurações do LANDesk NAC no console, é necessário ter pelo menos um servidor de correção e credenciais de usuário configuradas.

NOTA: A publicação inicial deve incluir todas as configurações
A primeira vez que você publica as configurações do NAC para os servidores de validação de postura e servidores de correção, é necessário incluir *todas* as configurações de validação do NAC, incluindo: conteúdo do NAC e arquivos de infra-estrutura (veja adiante os detalhes sobre esses arquivos). A publicação subsequente pode incluir o conteúdo do NAC ou somente as regras de conformidade. Em geral, os arquivos de infra-estrutura só precisam ser publicados uma vez nos servidores de correção.

Para publicar os parâmetros do NAC

1. Acesse a caixa de diálogo **Publicar configurações do NAC** e publique as configurações de vários locais na ferramenta Patch e conformidade. Por exemplo, clique com o botão direito no objeto **Controle de acesso de rede** ou no grupo **Conformidade** e depois clique em **Publicar**. O botão **Publicar** também é encontrado nas caixas de diálogo **Configurar NAC** e **Configurar o servidor de correção**. Além disso, você pode clicar no botão da barra de ferramenta **Publicar configurações NAC**.


Publicar configurações do Controle de acesso à rede
Selecione as configurações do Controle de acesso à rede da LANDesk que deseja publicar para os servidores posture de validação e de reparo.
Todos
Conteúdo do LANDesk NAC
Infra-estrutura
Arquivos de suporte e instalação
Páginas HTML
Reparar o cliente roaming 802.1x
OK
Cancelar
Ajuda

2. Para publicar todas as configurações do NAC, inclusive o conteúdo do LANDesk NAC e os arquivos de infra-estrutura para todos os servidores de validação de postura e de correção de uma só vez, selecione a caixa de seleção **Todas** e clique em **OK**.
3. Se quiser publicar apenas o conteúdo do NAC (definições de segurança, as configurações do NAC, regras de conformidade ou patches associados) para os servidores de validação de postura e de correção, selecione a caixa de seleção **Conteúdo do NAC** e clique em **OK**.
4. Se quiser publicar apenas os arquivos de infra-estrutura (análise de cliente de segurança, instalações de agentes confiáveis e páginas HTML para os servidores de correção), marque a caixa de seleção **Infra-estrutura** e clique em **OK**. (Em geral, os arquivos de infra-estrutura só precisam ser publicados uma vez nos servidores de correção.)

Sobre a caixa de diálogo Publicar parâmetros NAC

Use esta caixa de diálogo para publicar as configurações do NAC nos servidores de validação de postura e para publicar configurações de correções (recursos) nos servidores de correção da sua rede.

- **Todos:** São publicados os parâmetros de conteúdo do NAC e os arquivos de infra-estrutura nos servidores apropriados.

- **Conteúdo NAC:** Publica os parâmetros e o conteúdo do NAC definidos na ferramenta Patch e conformidade em todos servidores de validação de postura e de correção que foram adicionados à rede.
  Importante: É necessário pelo menos um servidor de validação de postura na sua rede para publicar o conteúdo do NAC.
  O conteúdo do NAC representa as definições de vulnerabilidades e outros tipos de conteúdo de segurança que atualmente residem no grupo **Conformidade** da ferramenta Patch e conformidade, assim como as configurações do LANDesk NAC, como parâmetros de postura de estado de funcionamento e de conformidade, níveis de login etc., que são definidos na caixa de diálogo **Configurar parâmetros do LANDesk NAC**. As definições de segurança, postura de estado de funcionamento e não funcionamento e níveis de login são publicados nos servidores de validação de postura, e os arquivos de patch associados são publicados nos servidores de correção (com base no conteúdo do grupo Conformidade no momento da publicação).
  (**NOTA:** Se você alterar o conteúdo do grupo **Conformidade** ou mudar os parâmetros do NAC na caixa de diálogo **Configurar NAC**, será necessário publicar novamente esses dados nos seus servidores.)
- **Infra-estrutura:** Publica os seguintes recursos de correção em todos os servidores de correção adicionados à sua rede.
  - **Configuração e suporte de arquivos:** Os arquivos de configuração e suporte também representam a análise do cliente de segurança e as instalações de agente de segurança. O analisador do cliente de segurança que realiza análises de segurança e correção em dispositivos.
  - **Páginas HTML:** Representa as páginas modelo HTML que são servidas pelo servidor de correção aos dispositivos com agentes confiáveis instalados que estão tentando acessar a rede corporativa. Essas páginas informam o usuário final o que fazer a fim de ganhar acesso limitado à rede ou os instruem a corrigir os computadores para torná-los conformes com a diretiva de segurança e ganhar pleno acesso à rede corporativa. Essas páginas HTML são modelos que podem ser modificados. (**NOTA:** Em geral, os arquivos de Infra-estrutura só precisam ser publicados uma vez nos servidores de correção. Ao contrário do conteúdo do NAC (critérios de conformidade), não é necessário republicar esses arquivos toda vez que se mudar a diretiva de segurança de conformidade.

Usar as páginas de correção pré-definidas

As páginas de reparos do NAC são arquivos HTML publicados para servidores de correção com a ferramenta Publicar configurações do NAC no console. Essas páginas de reparos são parte dos arquivos de infra-estrutura de correção. Em geral, esses arquivos só precisam ser publicados uma vez nos servidores de correção.

Os arquivos HTML estão localizados na seguinte pasta no servidor núcleo:

ManagementSuite\Install\TrustedAccess\RemediationServer

As páginas HTML são simplesmente modelos e você deve modificá-los para satisfazer as suas próprias necessidades e requisitos de segurança de conformidade . Para obter mais informações sobre como personalizar as páginas HTML, consulte "Personalizar as páginas de correção" na página 542.

As seções abaixo descrevem os objetivos de cada página HTML.

Página de status de funcionamento

Esta página HTML deve ser usada para informar o usuário corporativo de um dispositivo que se conecta, que a postura desse dispositivo foi avaliada e o dispositivo é considerado em estado de funcionamento, de acordo com as credenciais de segurança de conformidade, e que recebeu pleno acesso à rede corporativa.

O nome desta página HTML é: Healthy.html

A página de status de funcionamento será exibida *somente* quando um dispositivo mudar de não funcionamento para funcionamento. Ela não será mostrada toda vez que um dispositivo aparecer como em funcionamento.

O URL para essa página no servidor de correção deve ser digitado no campo **URL em estado de funcionamento** quando for configurado um servidor de correção.

Página de status de visitante de primeira visita:

Esta página é usada para informar um usuário que se conecta a sua rede corporativa pela primeira vez que você implementou a segurança de conformidade ou de controle de acesso de rede e que ele terá a opção de navegar na Web (apenas acesso à Internet) ou deixar seu computador passar por uma análise de vulnerabilidades ou de riscos de segurança e correção, se necessário, antes de receber permissão de acesso à rede. Esta página fornece links que permitem acesso à Internet apenas ou que permite ao visitante descarregar e instalar o software necessário para a análise de conformidade e correção para que o dispositivo possa receber permissão de pleno acesso à rede.

O nome desta página é: Visitor.html

Esta página fornece links que permitem ao usuário conceder acesso à Internet apenas ou permite descarregar e instalar o agente confiável necessário para a correção, para que o dispositivo possa ser reparado, reanalisado e receber permissão de acesso total à rede.

O URL para essa página no servidor de correção deve ser digitado no campo **URL de visitante de primeira vez** quando for configurado um servidor de correção.

Página de status de funcionário com mal funcionamento

Esta página HTML é usada para informar o usuário final do dispositivo sendo conectado que este foi analisado e não satisfaz as credenciais de segurança de conformidade, é considerado em não funcionamento e foi negado o acesso à rede. O administrador de rede deve personalizar essa página HTML para que ela possa mostrar que vulnerabilidades ou outras exposições da segurança foram detectadas no dispositivo e fornecer instruções específicas sobre como corrigi-las. Quando o dispositivo for reparado, o usuário final deve conectar-se à rede outra vez para receber acesso.

O nome desta página é: FailedEmployee.html

O URL para essa página no servidor de correção deve ser digitado no campo **Funcionário falhou ao conectar ao URL** quando for configurado um servidor de correção.

Página de status de visitante com mal funcionamento

Esta página HTML é usada para informar o visitante da rede corporativa que seu dispositivo foi analisado e não satisfaz as credenciais de segurança de conformidade, e foi negado o acesso à rede. Como no caso da página de status de mau funcionamento do funcionário, os administradores de rede podem personalizar essa página HTML para que ela possa mostrar que vulnerabilidades ou outras exposições da segurança foram detectadas no dispositivo e fornecer instruções específicas sobre como corrigi-las. Quando o dispositivo for reparado, o visitante deve clicar no ícone a Análise de segurança para acesso à rede que aparece na desktop.

O nome desta página é: FailedVisitor.html

O URL para essa página no servidor de correção deve ser digitado no campo **Visitor falhou ao conectar ao URL** quando for configurado um servidor de correção.

Personalizar as páginas de correção

Como mencionado anteriormente, as páginas HTML de correção são simplesmente modelos que podem ser editados e modificados manualmente para atender aos requisitos e diretivas específicos de segurança de conformidade.

Você pode usar qualquer editor de HTML para modificar arquivos HTML. Os textos existentes podem ser modificados de modo a fornecer informações úteis específicas adicionais à rede corporativa e adicionar seções DIV HTML para as definições de segurança que estão contidas na diretiva de segurança de conformidade (isto é, as definições contidas no grupo **Conformidade** na ferramenta Patch e conformidade).

Lembre-se que, se mudar o arquivo HTML no servidor núcleo após sua publicação nos servidores de correção, será necessário publicar novamente os arquivos nesses servidores antes que possam ser apresentados aos dispositivos de conexão (selecione **Páginas HTML** no grupo **Infraestrutura** da caixa de diálogo **Publicar configurações do NAC**).

Acréscimo de seções DIV para exibir dinamicamente as definições de segurança cuja correção falhou

Pode ser especialmente útil aos usuários finais corporativos e aos visitantes da sua rede, personalizar as páginas que "falharam" (ou estão em mau funcionamento) para poderem ver exatamente a natureza dos problemas de segurança e as etapas específicas que devem ser executadas a fim de corrigir o problema para o dispositivo ser reanalisado, considerado em bom funcionamento e receber pleno acesso à rede.

Essas páginas são destinadas a exibir dinamicamente o conteúdo quando a vulnerabilidade detectada não puder ser reparada pela ferramenta de correção da análise de segurança. Em outras palavras, se o dispositivo do usuário final for analisado e forem detectadas vulnerabilidades e outras exposições da segurança (por exemplo, ameaças de segurança à configuração do sistema, spyware, etc.) e a tarefa de reparo falhar, a página HTML que falhou (ou estiver em mau funcionamento) pode mostrar as definições específica de segurança identificadas pelos números de ID exclusivos junto com outras informações que instruem o usuário final a corrigir o problema *desde que* o administrador do sistema tenha adicionado a seção DIV para aquela definição de segurança (consulte o exemplo de seção DIV abaixo). Se a correção de uma definição de segurança falhar e essa definição não tiver uma seção DIV correspondente no arquivo HTML, não será mostrada nenhuma informação específica a essa definição no navegador do dispositivo do usuário final.

Para personalizar uma página de HTML

1. Abra o arquivo HTML no seu editor de HTML.
2. Edite os textos "boilerplate" existentes a fim fornecer as informações detalhadas que quiser que os usuários finais (funcionários corporativos e visitantes) vejam quando conectarem-se à rede corporativa.
3. Nas páginas HTML que falharam, adicione novas seções DIV no código HTML (usando os exemplos de seções DIV como modelo) para as definições de conteúdo de segurança que você colocou no grupo Conformidade que define a sua diretiva de segurança de conformidade.
   Não é necessário adicionar seções DIV para cada definição de segurança, mas somente as definições que têm seções DIV no arquivo HTML podem aparecer se a exposição da segurança for detectada *e* não for reparada pela análise de segurança. Veja o exemplo de DIV abaixo.
   Você pode adicionar etapas necessárias ao reparo do problema de segurança, links para sites de download de software e quaisquer outras informações que achar que auxiliarão o usuário final a resolver o problema.
4. Salve as mudanças.
5. Publique outra vez as páginas HTML nos servidores de correção.

O exemplo de entrada DIV é um arquivo HTML que falhou (em mau funcionamento)

Segue um exemplo de texto que apareceria no navegador se houvesse falha de conformidade na análise de segurança do dispositivo e se tivesse sido identificada com mau funcionamento. Esse exemplo é baseado no texto boilerplate já nos arquivos HTML com falha e descreve duas definições de segurança que não poderiam ser consertadas.

Atualização automática do Windows (ST000003):

Etapa 1: Clique em Iniciar

Etapa 2: Clique no Painel de controle

Etapa 3: Abra as Atualizações automáticas

Etapa 4: Clique em Automático

Etapa 5: Clique em OK

Não há software antivírus (AV-100): Clique aqui para instalar o cliente do Antivírus Symantec

E eis aqui o código HTML verdadeiro para aquele exemplo:

```
<div style="display:block;clear:both;"> </div>
<div id="ttip">
<p>
<ul>
<li>Etapa 1: Clique em Iniciar </li>
<li>Etapa 2: Clique no Painel de controle</li>
<li>Etapa 3: Abra as Atualizações automáticas</li>
<li>Etapa 4: Clique em Automática </li>
<li>Etapa 5: Clique em OK</li>
</ul>
</p>
</div>
<div id="ttip">
<p>
```

```
<strong>Nenhum antivírus (AV-100):</strong> <a href="symantec.exe"><strong>Clique aqui</strong></a>
para instalar o Symantec Anti-Virus Client
</p>
</div>
```

Busca e inserção de IDs de definição

A definição de segurança é identificada pelo seguinte código no arquivo HTML:

```
<div id="ttip">
```

Onde "ttip" é o ID real da definição de segurança. O ID de definição está na sua página de propriedades do Patch e conformidade. Digite o ID exatamente como aparece nas propriedades da definição.

Se houver falha no reparo dessa definição de segurança em particular, o conteúdo da seção DIV aparecerá dinamicamente no browser do usuário final e fornecerá ao usuário informações úteis para reparar o problema (de acordo com as informações que você inseriu).

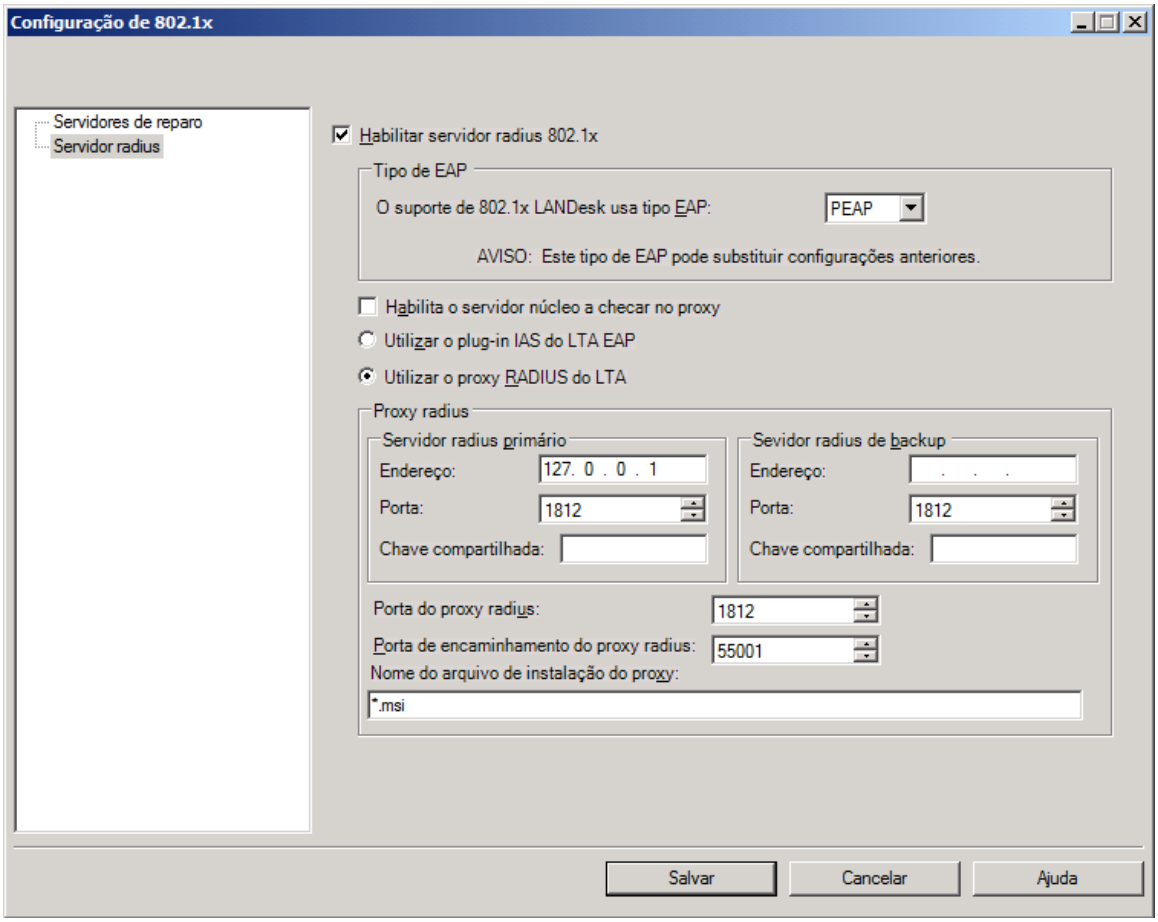
Primeiro, verifique se o suporte ao 802.1X NAC está habilitado

Após configurar e habilitar o suporte NAC 802.1X DE LANDesk na rede (veja a lista abaixo) e definir sua diretiva de segurança de conformidade você pode realizar tarefas contínuas de gerenciamento de segurança de conformidade descritas nos seguintes tópicos.

Lista de verificação do 802.1X NAC sendo habilitada

O suporte ao LANDesk 802.1X NAC está habilitado quando **TODAS** as condições a seguir existirem:

- **Dispositivo de controle à rede:** Deve ser instalado e configurado adequadamente com os serviços necessários em execução. No 802.1X NAC, este é o seu switch de rede e o servidor Radius 802.1X.
- **Ferramenta de Patch e conformidade:** Pode ser acessado no console por um usuário com as permissões necessários. (Você precisa também ter uma assinatura de conteúdo do Security Suite válida que permite descarregar conteúdo de segurança.)
- **Grupo de conformidade:** Contém ao menos uma definição do conteúdo de segurança. O conteúdo do grupo Conformidade é o fator primário que define a sua diretiva de segurança de conformidade e pode incluir vulnerabilidade de SO e aplicativo, spyware, antivírus, atualizações de software, definições personalizadas e ameaças de segurança de configuração do sistema. Se o grupo Conformidade estiver vazio, não há credenciais de segurança a serem verificadas, a validação de postura não pode ocorrer e o NAC não é operacional.
- **Servidor de correção:** Pelo menos um servidor de correção está instalado e configurado corretamente, com recursos de correção nele publicados vindo do servidor núcleo. (Recursos de correção incluem o cliente de segurança ou o utilitário analisador de vulnerabilidade, patches associados com as vulnerabilidade contidos no grupo Conformidade e as páginas HTML que fornecem links para instalar agentes confiáveis, realizar análises de segurança de conformidade e corrigir vulnerabilidades detectadas e outras exposições.)
- **Opção habilitar servidor Radius 802.1X:** Deve ser selecionado na caixa de diálogo **802.1X Configuration**.



Definir seu próprio nível de segurança de conformidade

Se todas as condições destacadas em "Lista de verificação do 802.1X NAC sendo habilitada" na página 544 forem satisfeitas, o suporte ao LANDesk 802.1X NAC está em execução na sua rede.

IMPORTANTE: O **LANDesk 802.1X NAC estende a segurança de um ambiente do servidor Radius 802.1X**
Lembre-se que a ferramenta LANDesk 802.1X NAC é projetada para ser compatível e para estender a segurança de uma implementação de servidor Radius 802.1X *existente* na sua rede. O suporte para LANDesk 802.1X NAC adiciona recursos de autenticação e conformidade para funcionalidade de controle de acesso básico de 802.1X.

É claro que há flexibilidade no serviço e você pode personalizar a forma como o NAC com os dispositivos, o que inclui opções como, por exemplo, Lista de exclusão e Permitir todos. Você também pode controlar o nível de segurança através de quantas e quais definições exatas de conteúdo de segurança coloca no grupo Conformidade, além do número de horas que especifica antes da execução automática da segurança de conformidade nos dispositivos conectados.

Ao ajustar essas opções e os critérios de diretiva, você pode definir diretivas de segurança muito estritas e complexas ou diretivas de segurança simples e permissíveis, ou qualquer nível entre as duas. Em outras palavras, você conta com a habilidade de personalizar o grau de dificuldade ou de facilidade com que um dispositivo que se conecta, conforma-se aos critérios de segurança que especificar.

Mais importante ainda é o fato de que pode mudar a natureza da sua diretiva de segurança de conformidade a qualquer momento a fim de satisfazer as circunstâncias e os requisitos que variam de forma constante. Lembre-se que toda vez que mudar o critério de segurança de conformidade (por exemplo, o conteúdo do grupo **Conformidade** em Patch e conformidade, você precisa publicar novamente as configurações do NAC para os servidores de validação de postura e servidores de correção. Para obter mais informações, consulte "Publicar as configurações de NAC em servidores" na página 538.

Modificar e atualizar diretivas de segurança de conformidade

É possível modificar e atualizar a sua diretiva de segurança de conformidade a qualquer momento.

Isso é feito mudando-se o conteúdo do grupo **Conformidade** na ferramenta Patch e conformidade.

Você precisa, então, publicar novamente o conteúdo do NAC nos servidores de validação e nos servidores de correção. Lembre-se que a publicação de conteúdo do NAC envia configurações do NAC e regras de conformidade aos servidores de validação de postura e a quaisquer patches associados aos servidores de correção, enquanto que a publicação de Arquivos de infra-estrutura envia arquivos de configuração e de suporte (inclusive o analisador do cliente de segurança, instalações do agente confiável e páginas modelo HTML) aos servidores de correção. (**NOTA:** Em geral, os arquivos de Infra-estrutura só precisam ser publicados uma vez nos servidores de correção. Ao contrário do conteúdo do NAC, não é necessário republicar esses arquivos toda vez que você mudar a diretiva de segurança de conformidade.

Para obter mais informações, consulte "Publicar as configurações de NAC em servidores" na página 538.

O que acontece em um dispositivo gerenciado configurados com o LANDesk 802.1X NAC

Quando um dispositivo gerenciado configurado com o LANDesk 802.1X NAC tenta se conectar à rede, tem lugar o seguinte processo:

1. Aparece um prompt de login solicitando nome de usuário e senha.
2. O usuário final precisa digitar as credenciais de autenticação corretas.
3. As credenciais são enviadas ao servidor Radius 802.1X (junto com os dados EAP) para iniciar a análise de segurança de conformidade no dispositivo do usuário final.
4. A análise de segurança de conformidade determina se o dispositivo é funcional (está em conformidade) ou não funcional (fora de conformidade) de acordo com a sua diretiva de segurança personalizada.

   Se o dispositivo analisado estiver funcional é concedido o acesso dele à rede corporativa.

   OU

   Se o dispositivo analisado estiver com mal funcionamento, ele é colocado na rede de quarentena onde será corrigido (através do atalho Correção na área de trabalho do dispositivo) e analisado novamente para obter acesso à rede corporativa.

Para encontrar uma descrição mais detalhada do fluxo de trabalho do processo de autenticação e conformidade e como os diferentes componentes interagem, consulte "Fluxos de processo, topologia de rede e componentes 802.1X NAC" na página 519.

IMPORTANTE: Reconfiguração manual da autenticação do 802.1X no dispositivo do usuário final
Se a autenticação falhar mesmo se você tiver certo de que as credenciais de login corretas foram inseridas, você pode reiniciar a placa de rede local para forçar outra tentativa de autenticação. No dispositivo gerenciado, clique em **Iniciar > LANDesk > redefinir 802.1X**.

Ao executar a opção de redefinir o 802.1X, certifique-se de primeiro fechar qualquer caixa de diálogo aberta do Windows, caso contrário a caixa de diálogo de login não será exibida. Se a caixa de diálogo de login desaparecer muito depressa, provavelmente isso é causado pelo término do tempo limite do LINK-3-UPDOWN e simplesmente tente redefinir 802.1X novamente.

Exibir dispositivos fora de conformidade

Você pode ver quais dispositivos foram colocados em postura e descobriu-se que estão com mau funcionamento ou fora de conformidade,

Para exibir dispositivos fora de conformidade

1. Na ferramenta Patch e conformidade, clique no botão **Computadores fora de conformidade** da barra de ferramentas. Ou clique o botão direito no grupo **Conformidade** e, em seguida, clique em **Computadores afetados**.
2. Uma caixa de diálogo é exibida com os dispositivos fora de conformidade.
3. Selecione um dispositivo na lista para exibir as definições de segurança com as quais o dispositivo é vulnerável ou fora de conformidade.

Solução de problemas do LANDesk 802.1X NAC

Essa seção contém informações sobre alguns problemas que podem ocorrer com o LANDesk 802.1X NAC e como resolvê-las.

A tarefa programada de análise de segurança de conformidade retorna o status de "conexão perdida"

Se uma tarefa programada de análise de segurança de conformidade do 802.1X retorna um status "conexão perdida" com o dispositivo alvo ou "tarefa falhou", pode ser porque o status da tarefa foi enviado ao servidor núcleo enquanto a máquina era reiniciada. Se você vir esse status, pode verificar o dispositivo alvo para ver se está ou não em quarentena.

Com um switch Huawei, vários prompts de login no 802.1X são exibidos

Ao usar um switch Huawei de 2 camadas (série H3C S3900), se o dispositivo exibir mais de um prompt de login do 802.1X e o usuário final cancelar ou fechar um deles sem digitar as credenciais corretas, o processo de autenticação do 802.1X é cancelado. Nesse caso, os usuários devem digitar as credenciais corretas em cada prompt de login. Se a autenticação for cancelada, use a opção de menu de redefinição do 802.1X para reiniciar o processo de autenticação.

Com um dispositivo Windows XP SP2, a autenticação inicial falha após a correção

Se corrigir um dispositivo não funcional de usuário final que estiver executando o Windows XP SP2 e a subsequente autenticação falhar, você pode usar a opção do menu de redefinição do 802.1X para iniciar o processo de autenticação e acessar com sucesso a rede corporativa.

Se o servidor Radius não estiver disponível, a autenticação do dispositivo falha

Em uma situação onde o servidor Radius 802.1X não está disponível para se comunicar com o agente LTA EAP em um dispositivo de usuário final, o dispositivo é colocado na rede de quarentena mas não tem a configuração correta, portanto ele não pode ser corrigido e não pode autenticar. Você precisa aguardar até o servidor Radius estar disponível e então usar a opção de menu de redefinição do 802.1X no dispositivo para reiniciar o processo de autenticação.

O 802.1X foi desenvolvido para trabalhar somente em plataformas desktop

O 802.1X não é suportado por plataformas de servidores.

Patch e conformidade

Visão geral do Patch e conformidade

Patch e conformidade é uma solução de gerenciamento de segurança integrada que ajuda a proteger seus dispositivos gerenciados LANDesk de uma variedade de riscos prevalentes de segurança e exposições.

Patch e conformidade fornece todas as ferramentas que você precisa para descarregar os tipos mais comuns de atualizações de conteúdo de segurança (com vulnerabilidade, spyware, ameaças de segurança de configuração, arquivos de definição de vírus (padrão) e aplicativos não autorizados) dos serviços de segurança do LANDesk. Você pode descarregar arquivos de patch associados e configurar e executar análises de avaliação de segurança e correção nos dispositivos gerenciados. Permite também criar as suas próprias definições personalizadas de segurança para analisar e corrigir dispositivos para condições específicas prejudiciais em potencial. Se forem detectados riscos de segurança, o Patch e conformidade fornece uma variedade de métodos para corrigir dispositivos afetados. Além disso, você pode ver as informações detalhadas de segurança para dispositivos analisados e gerar relatórios especializados de patch e conformidade.

Todas essas tarefas de gerenciamento de segurança de empresa podem ser realizadas na conveniência de um console.

Além disso, o Patch e conformidade permite analisar dispositivos gerenciados e servidores núcleo e computadores consoles, para versões do software do LANDesk instalado e distribuir as atualizações de software LANDesk adequadas.

NOTA: Sobre a LANDesk Security Suite
A Ferramenta de Patch e conformidade é o principal componente de gerenciamento de segurança do LANDesk Security Suite. O Security Suite é baseado na maior parte da funcionalidade primária do LANDesk Management Suite, suplementado com ferramentas de gerenciamento de segurança especializada como Patch de conformidade, Antivirus, Segurança de ponto final (HIPS, Firewall, Controle de dispositivo) e muito mais. A ferramenta Patch e conformidade oferece os mesmo recursos no Management Suite e Security Suite e é descrito em detalhes nesta seção. Para obter mais informações sobre quais funcionalidades básicas do LANDesk são suportadas no Security Suite, consulte as seções do LANDesk Security Suite.

NOTA: A Comunidade de usuários da LANDesk
A Comunidade de usuários LANDesk tem fóruns de usuários e os melhores métodos conhecidos para todos os produtos e tecnologia da LANDesk. Para acessar esse recurso valioso, visite: Página inicial da Comunidade de usuários da LANDesk

No futuro: O que você deve fazer após configurar dispositivos para a análise de segurança e correção

Assim que compreender os conceitos do Patch e conformidade, como navegar na interface do usuário e no fluxo de trabalho das tarefas gerais e após ter configurado dispositivos para funcionar com o Patch e conformidade, você pode realizar as seguintes tarefas de patch e conformidade: Veja "Descrição das tarefas principais de Patch e conformidade" na página 552.

Tópicos relacionados

- "Requisitos e recursos do Patch e conformidade" na página 550
- "Descrição das tarefas principais de Patch e conformidade" na página 552
- "Tipos de conteúdo de segurança e assinaturas" na página 569
- "Entenda a administração baseada em funções com o Patch e conformidade" na página 553
- "Download das atualizações do conteúdo de segurança" na página 571
- "Visão geral de análises de segurança" na página 588
- "Visão geral da correção de segurança" na página 598
- "Exibir dados de segurança detectados" na página 596

Requisitos e recursos do Patch e conformidade

O Patch e conformidade oferece todas as ferramentas necessárias para estabelecer uma segurança de sistema em toda a rede. Com o Patch e conformidade, você pode automatizar os processos repetitivos de manter o conteúdo de segurança e patch e organizar e ver esse conteúdo.

Use as tarefas de análise de segurança e diretivas para acessar dispositivos gerenciados para conhecidas vulnerabilidades específicas a plataformas. Você pode obter por download e gerenciar arquivos executáveis de patch. Finalmente, pode corrigir as vulnerabilidades detectadas ao distribuir e instalar os necessários arquivos patch e verificar a correção bem sucedida.

Você também pode criar suas próprias definições de vulnerabilidade a fim de analisar dispositivos gerenciados para condições específicas de SO e de aplicativo, que possam ameaçar a operação e segurança do sistema. Definições personalizadas podem ser configuradas para detecção somente ou para detecção e correção.

Caracterísicas básicas

Com o Patch e conformidade, é possível:

- Fornecer segurança de correção para versões internacionais dos sistemas operacionais na rede, incluindo suporte para os seguintes idiomas: tcheco, dinamarquês, holandês, inglês, finlandês, francês, alemão, italiano, japonês, norueguês, polonês, português, chinês simplificado, espanhol, sueco e chinês tradicional.
- Organizar e agrupar definições de segurança para executar avaliação e correção de segurança personalizada.
- Avaliação de vulnerabilidades e outros riscos de segurança em uma variedade de plataformas suportadas de dispositivos, inclusive Windows, Sun Solaris e Linux.
- Exibir as informações de segurança e patch dos dispositivos analisados
- Agendar tarefas automáticas de gerenciamento de correções, como atualizações de conteúdo, análise de dispositivos e downloads de correções.
- Realizar correções como uma tarefa agendada, uma diretiva ou automaticamente com o recurso Correção Automática.
- Descarregar, distribuir e instalar patchs que foram pesquisados e verificados.
- Controlar o status de distribuições e instalações de correções em dispositivos analisados.

- Usar os recursos de Multidifusão dirigida, download de parceiro e reinício do ponto de verificação da LANDesk para uma distribuição rápida e eficiente de correções.
- Gerar e exibir uma grande variedade de relatórios de patch e conformidade específicos de gerenciamento.

Características melhoradas

Patch e conformidade oferece vários novos recursos como:

- Use a tarefa de mudança de definições para mudar/atualizar apenas as definições de configuração de agente que desejar, incluindo: configurações de suporte de 802.1X, configurações de segurança de conformidade, configuração de definições de firewall do Windows, configurações de substituição de variável personalizada, configurações de HIPS, configurações de LANDesk Antivirus e análise de segurança e configurações de reparo. Com a tarefa de mudança de definições você pode mudar as definições desejadas sem uma distribuição de configuração completa de agente de dispositivo.
- Configurações de alerta globais.
- Fazer análise para verificar a presença de spyware nos seus dispositivos gerenciados. Se um spyware for detectado, é possível agendar um trabalho de reparo que remove o spyware dos dispositivos afetados.
- Negar o uso de aplicativos não autorizados ou proibidos nos dispositivos dos usuários finais com definições de aplicativos bloqueados.
- Habilitar a monitoração de spyware em tempo real (detecção e remoção) e bloqueio de aplicativo em tempo real.
- Analisar dispositivos gerenciados para ameaças de segurança (erros e exposição da configuração do sistema Windows) na unidade de disco rígido local. Assim que uma ameaça de segurança é identificada, você pode efetuar o reparo necessário manualmente no dispositivo afetado.
- Use específicas definições de ameaça de segurança disponíveis que permitem detectar a firewall do Windows, ligá-las ou desligá-las e configurar os respectivos parâmetros.
- Usar variáveis personalizadas incluídas com outras definições de ameaça de segurança a fim de personalizar e mudar configurações específicas de sistema local e fazer cumprir diretivas de configuração de sistema da empresa inteira.
- Receber alertas quando as vulnerabilidades especificadas forem detectadas em dispositivos gerenciados pela análise de segurança. Você pode configurar alertas por gravidade da definição.
- Implementar freqüentes análises segurança para riscos de segurança críticos e cronológicos como análise de vírus.
- Usar o relacionamento de dependência para identificar quais patches precisam ser instalados antes que outras vulnerabilidades possam afetar de maneira adversa os dispositivos gerenciados ou antes de eles puderem ser corrigidos. Informações sobre substituição descrevem patches que foram substituídos por versões mais recentes e que não precisam ser aplicados.
- Verificar a existência do software LANDesk mais recente instalado nos dispositivos gerenciados assim como nos servidores núcleo e consoles fazendo uma análise para detectar atualizações do software LANDesk. Se for detectada uma versão desatualizada em um dispositivo, você pode agendar um trabalho de reparo que distribui e instala a atualização mais recente do software LANDesk.

Plataformas de dispositivo com suporte

O Patch e conformidade suporta a maioria das plataformas de dispositivo padrão gerenciadas pelo LANDesk, inclusive os seguintes sistemas operacionais:

- Windows NT 4.0 (SP6a e superior)
- Windows 2000 Profissional (SP4)
- Windows 2003 Servers
- Windows XP Profissional (SP1/SP2/SP3)
- Windows Vista
- Mac OS X (10.2.x, 10.3.x, e 10.4.x)
- Red Hat Linux 9 (análise usando o console; correção manual)
- SUSE Linux (análise usando o console, correção manual)
- Sun Solaris (análise usando o console, correção manual)

Para obter informações sobre a configuração de dispositivos gerenciados para análise de segurança, consulte "Configurar dispositivos para análise de segurança e correção" na página 563.

IMPORTANTE: A análise dos servidores núcleo e consoles para atualizações de software LANDesk é suportada
É possível analisar também servidores núcleo LANDesk e consoles para as atualizações de software LANDesk, mas eles precisam antes receber a distribuição do agente padrão LANDesk, que inclui o agente do analisador de segurança requerido para as tarefas de análise de segurança.

Tópicos relacionados

"Patch e conformidade" na página 549

"Descrição das tarefas principais de Patch e conformidade" na página 552

"Entenda a administração baseada em funções com o Patch e conformidade" na página 553

"Download das atualizações do conteúdo de segurança" na página 571

"Visão geral de análises de segurança" na página 588

"Visão geral da correção de segurança" na página 598

"Exibir dados de segurança detectados" na página 596

Descrição das tarefas principais de Patch e conformidade

A lista abaixo descreve as principais tarefas envolvidas na configuração, implementação e uso do Patch e conformidade. Consulte os tópicos de ajuda específicos do recurso para obter informações conceituais e práticas detalhadas.

- Configure os dispositivos gerenciados para análises de segurança e reparo com o agente de análise de segurança (através da configuração do agente ou das tarefas de instalação/atualização).
- Descarregue o conteúdo de segurança (vulnerabilidade e outras definições de risco de segurança) de um servidor de conteúdo de segurança (atualizado das fontes de dados da indústria/fornecedor).

- Crie definições de vulnerabilidades personalizadas se desejar.
- Organize veja o conteúdo de segurança que foi baixado.
- Crie análises de avaliação de segurança e conformidade
- Configure definições de análise e reparo para determinar a operação do scanner e as opções do usuário final. (Essas configurações de análise e reparo definem suas diretivas de conformidade com a segurança.)
- Analise, com suas tarefas e configurações de análise personalizadas, dispositivos alvo para verificar a existência de vulnerabilidades, spywares, ameaças de segurança, aplicativos bloqueados etc.
- Veja os resultados da análise antivírus dos dispositivos analisados.
- Faça o download de patches (usado para remediar vulnerabilidades detectadas).
- Reparo de vulnerabilidades detectadas distribuindo e instalando patches em dispositivos afetados
- Corrija outros riscos de segurança detectados em dispositivos gerenciados.
- Ver o status da instalação do patch e informações do histórico de reparo.
- Gere relatórios específicos de segurança.

Tópicos relacionados

"Patch e conformidade" na página 549

"Requisitos e recursos do Patch e conformidade" na página 550

"Tipos de conteúdo de segurança e assinaturas" na página 569

"Entenda a administração baseada em funções com o Patch e conformidade" na página 553

"Download das atualizações do conteúdo de segurança" na página 571

"Visão geral de análises de segurança" na página 588

"Visão geral da correção de segurança" na página 598

"Exibir dados de segurança detectados" na página 596

Entenda a administração baseada em funções com o Patch e conformidade

O Patch e conformidade usa a administração baseada em funções (RBA) para permitir o acesso dos usuários aos recursos. A administração com base em funções é a estrutura de acesso e segurança que permite aos administradores LANDesk restringir o acesso a ferramentas e dispositivos. Cada usuário recebe funções e escopo específicos que determinam quais recursos podem usar e quais dispositivos podem gerenciar.

Os Administradores atribuem essas funções a outros usuários com a ferramenta Gerenciar usuários no console. Patch e conformidade é uma permissão específica que aparece no grupo Permissões de segurança na caixa de diálogo Funções. Para ver e usar a ferramenta Patch e conformidade, deve ser atribuído ao usuário o direito Patch e conformidade necessário.

IMPORTANTE: P**ermissões de grupos LANDesk Script Writers são necessárias**
Para criar tarefas agendadas e diretivas na ferramenta Patch e conformidade e a ferramenta

Configurações de segurança (para tarefas de análise de segurança e conformidade, tarefas de reparo e tarefas de mudanças de configurações), um usuário precisa ter permissão de grupo LANDesk Script Writers. Em outras palavras, eles precisam pertencer a um grupo que tenha permissão de LANDesk Script Writers atribuída. Para obter mais informações sobre a administração baseada em funções, consulte "Gerenciamento de usuários" na página 38.

Com o direito Patch e conformidade, você pode fornecer aos usuários a habilidade de:

- Ver e acessar a ferramenta Patch e conformidade no menu Ferramentas e na Caixa de ferramentas
- Configurar dispositivos gerenciados para análise de avaliação de segurança, conformidade e correção
- Configurar dispositivos para análise de spyware e aplicativo bloqueado em tempo real
- Configurar dispositivos para análise de alta freqüência para riscos críticos de segurança
- Obter por download as atualizações de segurança (regras de definições e detecção) e patches associados para os tipos de segurança para as quais você tem assinatura de conteúdo do Security Suite
- Criar tarefas agendadas que obtém por download definições e/ou atualizações de patches automaticamente
- Criar definições de vulnerabilidade personalizadas e regras de detecção personalizadas
- Importar, exportar e apagar definições personalizadas
- Exibir o conteúdo de segurança baixado por tipo (incluindo: todos os tipos, aplicativos bloqueados, definições personalizadas, atualização da LANDesk, ameaças à segurança, spyware, vulnerabilidades, atualização de driver e de software)
- Personalizar ameaças de segurança selecionadas com variáveis personalizadas
- Editar valores variáveis personalizados (para tipos de conteúdo de segurança com variáveis personalizadas como, por exemplo, ameaças de segurança)
- Adicionar e remover definições de segurança do grupo Conformidade
- Alterar o status das definições contidas no grupo Conformidade
- Configurar e executar análises de segurança e conformidade em dispositivos gerenciados como tarefa agendada ou como diretiva
- Dividir uma análise de tarefa agendada em uma fase de estágio e uma fase de distribuição
- Criar e configurar parâmetros de análise e reparo que determinam as opções de análise como: tipo de conteúdo a ser analisado, informações do analisador e indicação de andamento, comportamento de reinicialização de dispositivo e a quantidade de interação de usuário final. Aplique, então, os parâmetros de análise e reparo às tarefas de análise de segurança, tarefas de reparo, tarefas de desinstalação e tarefas de reinicialização
- Exibir resultados detalhados de análise por grupo detectado, definição específica, dispositivo individual ou por grupo de dispositivos selecionados
- Executar correção como uma tarefa agendada ou como uma diretiva
- Use o Reparo automático para corrigir automaticamente os seguintes tipos de segurança se forem detectados: vulnerabilidades, spyware, atualizações de software LANDesk e definições personalizadas (é necessário também ser um Administrador LANDesk).
- Controlar e verificar o status de distribuições e instalações de patches (histórico de reparos) em dispositivos analisados.
- Purgar definições de tipo de segurança não utilizadas (é necessário ser um Administrador LANDesk)
- Desinstalar patches de dispositivos analisados

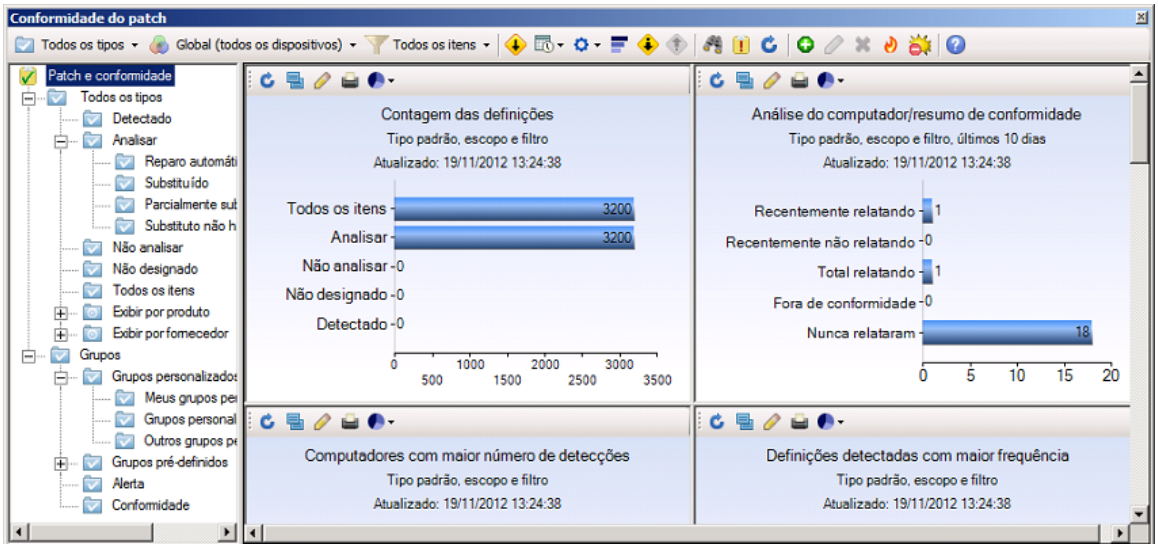
- Remover patches do banco de dados núcleo
- Configurar alertas de vulnerabilidades
- Gerar uma variedade de relatórios específicos de segurança (também requer as funções de Relatórios)

Entenda e use a Janela da ferramenta de Patch e conformidade

A Janela da ferramenta de Patch e conformidade, como todas as outras ferramentas LANDesk, é aberta no menu Ferramentas ou da Caixa de ferramentas e pode ser fixada, movida e alternada com outras janelas de ferramentas abertas.

IMPORTANTE: Permissão Patch e conformidade
Permite ver e acessar a ferramenta Patch e conformidade, os usuários precisam ter permissão de administrador LANDesk (permissões completas) ou a permissão específica Patch e conformidade. Para obter mais informações sobre funções e permissões do usuário, consulte "Gerenciamento de usuários" na página 38.

Para abrir a ferramenta Patch e conformidade, clique em **Ferramentas > Segurança e Conformidade > Patch e conformidade**.



A janela do Patch e conformidade contém uma barra de ferramentas e dois painéis. O painel esquerdo mostra uma árvore hierárquica dos grupos de definição de tipo e detecção de regras. É possível expandir ou recolher os objetos conforme necessário.

O painel do lado direito mostra uma lista em coluna, dos detalhes de definição dos grupos selecionados ou detalhes da regra de detecção, dependendo de qual grupo você selecionou no painel esquerdo além de um recurso Localizar para procurar nas listas longas de itens.

NOTA: Caracteres não permitidos ao procurar na lista
Na caixa **Localizar**, os seguintes caracteres estendidos não são suportados: <, >, ', ", !

Botões da barra de ferramentas

A janela da ferramenta Patch e conformidade contém uma barra de ferramentas com os seguintes botões:

- **Todos os tipos:**
- **Global (todos os dispositivos):**
- **Todos os itens:**
- **Download de atualizações:** Abre uma caixa de diálogo onde você pode especificar as plataformas e idiomas para os tipos de conteúdo de segurança que quiser atualizar, assim como qual servidor de conteúdo de segurança do LANDesk a acessar. Também é possível configurar se serão colocadas definições no grupo Não atribuída, se haverá um download dos patches associados simultaneamente, o local onde os patches são colocados e as configurações do servidor proxy.
- **Criar uma tarefa:** Inclui uma lista suspensa onde você pode selecionar o tipo de tarefa que deseja criar:
    - **Análise de segurança:** Permite criar uma tarefa de análise de segurança, especificar se a análise é uma tarefa agendada ou uma diretiva e selecionar configurações de análise e reparo que determinam a exibição da análise de segurança, o comportamento de reinicialização e a interação e os tipos de conteúdo analisados.
    - **Análise de conformidade:** Permite criar uma tarefa de análise de segurança que verifica especificamente os dispositivos alvo para conformidade com a sua diretiva atual de segurança conforme definida nas configurações do LANDesk Network Access Control e pelo conteúdo do grupo Conformidade. É também possível especificar se a análise de segurança e conformidade é uma tarefa agendada (incluindo quais dispositivos serão analisados e se a análise deve ser feita imediatamente) ou uma diretiva.
    - **Mudar configurações:** Permite criar uma tarefa que muda as configurações padrão em um dispositivo gerenciado gravando o ID das configurações especificadas no registro local. Com a tarefa de mudança de definições você pode mudar uma ou mais das seguintes: configurações de suporte de 802.1X, configurações de segurança de conformidade, configuração de definições de firewall do Windows, configurações de substituição de variável personalizada, configurações de HIPS, configurações de LANDesk Antivirus e análise de segurança e configurações de reparo. Você pode usar esta tarefa como um meio rápido e conveniente de mudar apenas as configurações que deseja sem ter que redistribuir uma configuração completa de agente de dispositivo.
    - **Reinicializar:** Permite criar uma tarefa de reinicialização do dispositivo, especificar se a reinicialização é uma tarefa agendada ou uma diretiva e selecionar a configuração de análise e reparo que determina o comportamento de exibição e interação. Observe que somente as opções na página de reinicialização da caixa de diálogo se aplica a essa tarefa.
    - **Reparar:** Permite criar uma tarefa de reparo de segurança que corrige exposições de segurança detectadas em dispositivos analisados. Você pode configurar o reparo como uma tarefa agendada ou como uma diretiva, ou como ambas, dividir a tarefa de reparo em estágios e fases de reparo separados, selecionar a configuração de análise e reparo e fazer o download de patches. Observe que uma ou mais definições de segurança precisar antes ser selecionadas para criar uma tarefa de reparo.
    - **Coletar informações de histórico:** Permite criar uma tarefa que coletar contagens de análise e detecção atuais (por número especificado de dias) que podem ser usadas para relatório. É também possível criar e configurar uma tarefa agendada que realiza a mesma ação.

- **Configurar definições:** Inclui uma lista suspensa onde você pode selecionar o tipo de definições que deseja configurar, mudar ou atualizar:
    - **Configurações de análise e reparo:** Permitem criar, editar, copiar e excluir definições configurações de análise e reparo. As configurações de análise e reparo determinam se a varredura de segurança é mostrada em dispositivos durante a execução, as opções de reinicialização, a interação do usuário e os tipos de conteúdo analisados.
    - **Definições de conformidade:** Permitem criar, editar, copiar e excluir definições de conformidade. As Definições de conformidade determinam quando e como ocorre uma análise de segurança e conformidade, se a correção é automática, e qual ação tomar quando o LANDesk Antivirus detecta uma infecção de vírus nos dispositivos alvo.
    - **Definições de substituição da variável personalizada:** Permitem criar, editar, aplicar e excluir configurações de análise e reparo. As substituições de variáveis personalizadas permitem configurar exceções para os valores de variáveis personalizadas. Em outras palavras, com essas definições você pode ignorar uma condição variável personalizada específica para que um dispositivo analisado não apareça como vulnerável.
    - **Configurações de grupo de definições:** Permite criar, editar, copiar e excluir configurações de grupo de definição para automatizar os downloads de conteúdo de segurança.
    - **Configurações de alerta:** permitem configurar alertas de segurança globais.
    - **Configurações de núcleo de rollup:** permitem criar e gerenciar configurações de núcleo de rollup. Configurações de núcleo de rollup determinam o encaminhamento automático dos resultados de análise de segurança mais recentes para um servidor de núcleo de rollup na sua rede. Análise de dados de segurança permite ver o status de vulnerabilidade em tempo real para todos os dispositivos gerenciados em uma grande rede empresarial distribuída sem ter que carregar manualmente os dados diretamente do servidor núcleo primário.
- **Criação de definições personalizadas:** Abre uma caixa de diálogo em branco, Propriedades de definição, com campos editáveis onde você pode especificar se a definição personalizada é apenas de detecção ou também permite correções, inserir informações específicas de vulnerabilidade, criar regras de detecção e identificar o arquivo patch apropriado para correção.
- **Importação de definições personalizadas:** Permite importar um arquivo XML contendo definições.
- **Exportação de definições personalizadas selecionadas:** Permite exportar uma definição personalizada com um arquivo XML.
- **Analisar informações:** permite ver informações de atividade e status de patch e conformidade por categorias como, análise recente e gravidade de definição, de todos os dispositivos gerenciados.
- **Computadores fora de conformidade:** Relaciona dispositivos que foram analisados para a verificação da conformidade com a diretiva de segurança de conformidade pré-definida (com base no conteúdo do grupo Conformidade), e são determinados fora de funcionamento e fora de conformidade.
- **Atualizar:** Atualiza o conteúdo do grupo selecionado.
- **Excluir definições personalizadas selecionadas:** Remove as definições personalizadas selecionadas do banco de dados núcleo.
- **Purgar definições de patch e conformidade:** Permite especificar as plataformas e os idiomas cujas definições deseja remover do banco de dados núcleo. **(IMPORTANTE:** Observe que apenas um usuário com direitos de Administrador LANDesk pode executar essa operação.)
- **Ajuda:** Abre a ajuda a seção Patch e conformidade.

Lista suspensa Tipo

Use a lista Tipo para determinar quais definições de download mostrar na exibição da árvore. Os tipos de definição são designados pelo autor da publicação do conteúdo. A filtragem da exibição pode ser muito útil se desejar ver somente um tipo específico de conteúdo de segurança, ou se desejar refinar uma lista extremamente longa.

A lista Tipo inclui as seguintes opções:

- Todos os tipos (lista compreensiva de todas as definições de segurança adquiridas por download)
- Antivírus (só relaciona as definições de detecção do analisador dos downloads; não contém os arquivos específicos de definições de vírus do LANDesk Antivirus)
- Aplicativos bloqueados (relaciona somente as definições de aplicativos bloqueados adquiridos por download)
- Definições personalizadas (relaciona somente definições de vulnerabilidade definidas pelo usuário)
- Atualizações de driver (relaciona somente definições de atualização de drivers obtidos por download)
- Atualizações do LANDesk (relaciona somente atualizações de software LANDesk)
- Ameaças de segurança (relaciona somente definições de ameaças de segurança obtidas por download)
- Atualizações de software (relaciona somente atualizações de software obtidas por download)
- Spyware (relaciona somente definições de spyware obtidas por download)
- Vulnerabilidades (relaciona somente todas as definições de vulnerabilidade obtidas por download para quaisquer plataformas disponíveis)

Tela da árvore

O objeto raiz da tela da árvore contém todos os tipos de segurança como, vulnerabilidades, spyware, ameaças de segurança, aplicativos bloqueados e grupos de definições personalizadas (e grupos associados de regra de detecção, se aplicável). O objeto raiz pode ser expandido e diminuído, conforme necessário. Os itens a seguir são exibidos no painel esquerdo da janela Patch e conformidade.

Todos os tipos (ou o nome do tipo selecionado no momento)

O objeto Todos os tipos contém os seguintes subgrupos:

- **Detectadas:** Relaciona todas as definições detectadas pelas análises de segurança para todos os dispositivos incluídos nas análises. O conteúdo deste grupo é cumulativo, baseado em todas as análises de segurança executadas na sua rede. As definições são removidas deste grupo somente se passarem por uma correção bem sucedida, forem removidas do grupo Analisar e se análise for executada novamente ou ao dispositivo afetado for removido do banco de dados.

  A lista Detectadas é um conjunto de todas as definições detectadas de segurança encontradas pela análise mais recente. As colunas Analisadas e Detectadas são úteis para mostrar quantos dispositivos foram analisados e em quantos desses dispositivos foram detectadas definições. Para ver especificamente em quais dispositivos foi detectada a definição, clique com o botão direito no item e clique em **Computadores afetados**.

  Observe que você também pode ver informações específicas do dispositivo clicando com o botão direito em um dispositivo na tela de rede e, em seguida, clicando em **Informações de Security e Patch**.

As definições podem ser movidas somente do grupo Detectadas para os grupos Não analisar ou Não atribuídas.

- **Analisar:** (Para o tipo Aplicativos bloqueados, este grupo é denominado **Bloco**.) Relaciona todas as definições de segurança que são pesquisadas quando o analisador de segurança é executado nos dispositivos gerenciados. Em outras palavras, se houver uma definição nesse grupo, ela fará parte da próxima operação de análise; caso contrário, ela não fará parte da análise.

  Como padrão, as definições coletadas são adicionadas ao grupo Analisar durante uma atualização do conteúdo. **(IMPORTANTE:** Por padrão, os aplicativos bloqueados são adicionados ao grupo Não atribuída.)

  A análise é um dos três estados possíveis para uma definição de segurança: Analisar, Não analisar e Não atribuída. Assim, uma definição pode existir em apenas um desses três grupos em um dado momento. Uma definição está no estado Analisar, Não analisar ou Não atribuída, e é identificada por um ícone exclusivo para cada estado: ponto de interrogação (?) para o estado Não atribuída, X vermelho para o estado Não analisar e o ícone regular de vulnerabilidade para o estado Analisar. Mover uma definição de um grupo para outro muda automaticamente seu estado.

  Ao transferir definições para o grupo Analisar (arraste uma ou mais definições de um outro grupo, com exceção do grupo Detectadas), você pode controlar a natureza e o tamanho específicos da próxima análise de segurança nos dispositivos alvo.

  CUIDADO: Mover definições do grupo Analisar
  Quando você move definições do grupo Analisar para o grupo Não analisar, as informações atuais contidas no banco de dados núcleo sobre quais dispositivos analisados detectaram essas definições são removidas do banco de dados núcleo e não ficam mais disponíveis no diálogo Propriedades ou na caixa de diálogo Informações do Security e Patch do dispositivo. Para restaurar essas informações de avaliação de segurança, você deve mover as definições de volta para o grupo Analisar e executar novamente uma análise de segurança.

- **Não analisar:** (Para Aplicativos bloqueados, este grupo é denominado **Não bloquear**.) Contém todas as definições que não serão pesquisadas na próxima vez em que o analisador de segurança for executado nos dispositivos. Conforme mencionado anteriormente, se uma definição estiver neste grupo, ela não poderá estar no grupo Analisar ou Não atribuída. Você pode mover as definições para este grupo para removê-las temporariamente de uma análise de segurança.
- **Não atribuídas:** Relaciona todas as definições que não pertencem aos grupos Analisar ou Não Analisar. O grupo Não atribuídas é basicamente uma área de armazenamento das definições coletadas até que você decida se elas devem ser analisadas ou não.

  Para mover as definições, arraste uma ou mais do grupo Não atribuídas para os grupos Analisar e Não analisar.

  Novas definições também podem ser adicionadas automaticamente ao grupo Não atribuídas durante uma atualização de conteúdo ao selecionar a opção **Colocar as novas definições no grupo Não atribuídas** na caixa de diálogo **Atualizar downloads**.

- **Todos os itens:** Contém todas as definições do tipo selecionado em uma lista simples, mesmo se uma definição para o grupo Não atribuída, Analisar ou Não analisar foi alterada.
- **Visualizar por produto:** Relaciona todas as definições organizadas em subgrupos de produto específicos. Esses subgrupos ajudam a identificar definições pela categoria produto.

Você pode usar esses subgrupos de produto para copiar definições no grupo Analisar incluídas para análise específica de produtos ou copiá-las em um grupo personalizado (veja abaixo para executar correções em grupos de produtos de uma só vez).

As definições podem ser copiadas de um grupo de produto ao grupo Analisar, Não analisar ou Não atribuída ou em qualquer grupo personalizado, definido pelo usuário. Elas podem residir simultaneamente em grupos de plataforma, produto e em vários grupos personalizados.

Grupos

O objeto Grupos contém os seguintes subgrupos:

- **Grupos personalizados:** Relaciona todos os subgrupos que você criou e as definições que eles contêm. Meus grupos constituem uma opção para organizar definições de segurança da maneira desejada. Use o conteúdo de um grupo para copiar várias definições no grupo Analisar para análise personalizada ou criar uma tarefa de reparo para várias definições de uma só vez.

  Você também pode usar um grupo personalizado para definir o conteúdo de uma análise de segurança. Copie as definições que quiser analisar no grupo personalizado e selecione esse grupo na opção Analisar por opções da caixa de diálogo Configurações de análise e reparo.

  Para criar um grupo personalizado, clique com o botão direito em **Grupos personalizados** (ou um subgrupo) e, em seguida, clique em **Novo grupo**.

  Para adicionar definições a um grupo personalizado, arraste uma ou mais delas de todos os outros grupos de definições. Você também pode clicar com o botão direito do mouse em um grupo personalizado e, em seguida, clicar em **Adicionar definições**.

- **Pré-definido:** Contém os grupos de definições de vulnerabilidade pré-definidos conforme determinados pela assinatura de conteúdo da LANDesk Security Suite. Por exemplo, este grupo pode conter definições publicadas pela indústria como, SANS Top 20, que são as 20 principais definições de vulnerabilidade identificadas e publicadas pela Microsoft. (Essas definições, em geral, são um subconjunto das Vulnerabilidades do Microsoft Windows que são obtidas por download com o uso da caixa de diálogo **Download de atualizações**.)
- **Alerta:** Relaciona todas as definições que gerarão mensagens de alerta na próxima vez em que o analisador de segurança for executado nos dispositivos.
- **Conformidade:** Relaciona todas as definições usadas para determinar se um dispositivo gerenciado (ou portátil/dispositivo convidado) está em estado de bom funcionamento ou não funcionamento (Healthy ou Unhealthy). Este grupo é usado pelo novo recurso LANDesk Network Access Control (NAC) para negar ou permitir acesso à rede principal. As definições e arquivos associados no grupo Conformidade são copiados para um servidor especial de correção que analisa dispositivos, determina conformidade ou não conformidade e pode corrigir dispositivos fora de conformidade de forma que eles possam receber acesso total à rede corporativa.

Regras de detecção

O grupo Regras de detecção mostra apenas certos tipos de conteúdo de segurança.

IMPORTANTE: Tipos de definições de segurança que usam regras de detecção
Estas regras de detecção definem as condições específicas (do sistema operacional, aplicativo, arquivo ou registro) verificadas por uma definição a fim de detectar o risco de segurança associado. Definições (ou seja, tipos de conteúdo) que usam regras de detecção incluem vulnerabilidades, ameaças de segurança, e definições personalizadas. Spyware e aplicativos bloqueados não usam regras de detecção.

O grupo Regras de detecção contém os seguintes subgrupos:

- **Analisar:** Relaciona todas as regras de detecção habilitadas para análise de segurança nos dispositivos.

  Por padrão, as regras de detecção associadas a uma definição de qualquer tipo de conteúdo de segurança são acrescentadas ao grupo Analisar regras de detecção durante uma atualização do conteúdo. Da mesma forma, as regras personalizadas de detecção associadas a definições personalizadas são acrescentadas ao grupo Analisar quando você cria a definição personalizada.

  Observe que além das regras de detecção de definições habilitadas, o arquivo patch executável correspondente da correção também deve ser obtido por download para um repositório local de patches na rede (normalmente o servidor núcleo) antes de ocorrer a correção. O atributo Downloaded (uma das colunas de detalhe no painel direito da janela da ferramenta) indica se a correção associada à regra foi carregada.

- **Não analisar:** Relaciona todas as regras de detecção desabilitadas para análise de segurança nos dispositivos. Algumas definições têm mais do que uma regra de detecção. Ao desabilitar uma regra de detecção, você assegura que ela não será usada para analisar as condições indicando que a definição está presente nos dispositivos. Isso lhe permite simplificar uma análise de segurança sem redefinir a definição.
- **Visualizar por produto:** Relaciona todas as regras de detecção para definições coletadas, organizadas em subgrupos específicos de produto. Esses subgrupos ajudam a identificar regras de detecção por sua categoria de produto relevante.

Use esses subgrupos de produtos para as operações de grupo.

Configurações

O grupo Configurações permite ver as várias configurações criadas para as tarefas de análise. Você pode clicar com o botão direito em qualquer grupo Configurações para criar novas configurações e ver as informações de configurações em um formato de relatório.

Contém os seguinte subgrupos:

- **Análise e reparo:** Contém todas as configurações de análise e reparo que você criou e que são usadas para definir a operação do analisador de segurança. As configurações de análise e reparo têm um número de ID exclusivo. O painel direito mostra informações úteis para as configurações de análise e reparo relacionadas.

- **Conformidade:** Contém todas as configurações de conformidade que você criou e que são usadas para definir a operação da análise de segurança ao realizar uma análise de conformidade específica. Cada configuração tem um número de ID exclusivo. O painel direito mostra informações úteis para as configurações de análise e reparo relacionadas.
- **Variáveis personalizadas a serem circunventadas:** Contém todas as configurações de circunvenção de variável personalizada criadas que são usadas para determinar os valores de variável personalizada a serem ignorados quando o analisador de segurança for executado. Cada configuração tem um número de ID exclusivo. O painel direito mostra informações úteis para as configurações relacionadas.

Detalhes da definição

O painel direito da janela do Patch e conformidade mostra informações detalhadas, relacionadas em colunas classificáveis, para itens de regra de definição e detecção, conforme descrito a seguir.

- **ID:** Identifica a definição com um código alfanumérico exclusivo, definido pelo fornecedor.
- **Gravidade:** Indica o nível de severidade da definição. Os níveis possíveis de gravidade são: Service Pack, Crítica, Alta, Média, Baixa, Não aplicável (N/A) e Desconhecida.
- **Título:** Descreve a natureza ou alvo da definição em um breve texto.
- **Idioma:** Indica o idioma do SO ou do aplicativo afetado pela definição.
- **Data de publicação:** Indica a data em que a definição foi publicada pelo fornecedor.
- **Reparável:** Indica se a definição pode ser consertada com a distribuição e instalação do arquivo de correção. Os possíveis valores são os seguintes: Sim, Não, Alguns (para uma definição que inclui regras múltiplas de detecção e nem todas as definições detectadas podem ser reparadas) e Nenhuma regra (para uma definição personalizada que não inclui regras de detecção).
- **Instalação silenciosa:** Indica se o arquivo do patch associado à definição (ou patches) será instalado silenciosamente, ou seja, sem interação com o usuário. Algumas definições podem ter mais de um patch. Se os patches das definições não forem instalados silenciosamente, o atributo de Instalação silenciosa dirá Não. Para ver como cada patch é instalado, clique com o botão direito na definição e, em seguida, clique em **Propriedades > Patches**.
- **Detectadas:** Mostra o número de dispositivos analisados que detectaram a definição.
- **Analisados:** Mostra o número de dispositivos analisados em relação à definição.
- **Correção automática:** Indica se o recurso Reparo automático está habilitado ou desabilitado para a definição.
- **ID do CVE:** (Aplica-se somente a vulnerabilidades) Identifica uma vulnerabilidade através do nome exclusivo CVE (Common Vulnerabilities and Exposures).

Detalhes da Regra de detecção

- **Nome:** Mostra o nome da regra de detecção (pode ser o nome do arquivo do executável de patch).
- **ID:** Mostra o ID da definição associada à regra.
- **Reparável:** Indica se a definição associada pode ser reparada com a distribuição e instalação do arquivo do patch.
- **Instalação silenciosa:** Indica se a regra do patch associado será instalado silenciosamente nos dispositivos sem interação com o usuário.
- **Reinicializar:** Indica se o arquivo patch associado requer uma reinicialização do sistema para completar uma correção com êxito.

- **Correção automática:** Indica se o recurso Correção automática está habilitado ou desabilitado para a definição associada.
- **Download pronto:** Indica se o arquivo executável de correção da regra foi obtido por download no repositório local.

Clique com o botão direito numa regra de detecção para ver mais detalhes com a opção **Propriedades**. O menu de atalho permite também habilitar/desabilitar a regra, descarregar o caminho associado, abrir a pasta de repositório de patch e desinstalar o patch.

Tarefas e opções do menu de atalho

Clique com o botão direito em uma definição para ver mais detalhes com a opção **Propriedades**.

Um menu de atalho de definição também permite realizar as seguintes tarefas (dependendo do tipo de segurança):

- Computadores afetados
- Computadores que não são analisados
- Download dos patches associados
- Reparo automático ao analisar
- Adicionar a um grupo de conformidade
- Adicionar a um grupo Alerta
- Limpar análise/status do reparo
- Reparar
- Copiar
- Propriedades
- Inf.
- Exportar
- Copiara para outro(s) núcleo(s)
- Sinc. automática

Configurar dispositivos para análise de segurança e correção

Antes que os dispositivos gerenciados possam ser analisados para a checagem de vulnerabilidades, spyware, ameaças de segurança e outros tipos de segurança, e receberem distribuições de patch ou atualizações de software, é necessário que o agente de análise de segurança esteja instalado (esse agente é instalado como padrão com o agente padrão LANDesk).

Esta seção inclui informações sobre a configuração de dispositivos Windows para a análise através de uma configuração de agente e informações sobre a configuração de dispositivos Linux, UNIX e Mac.

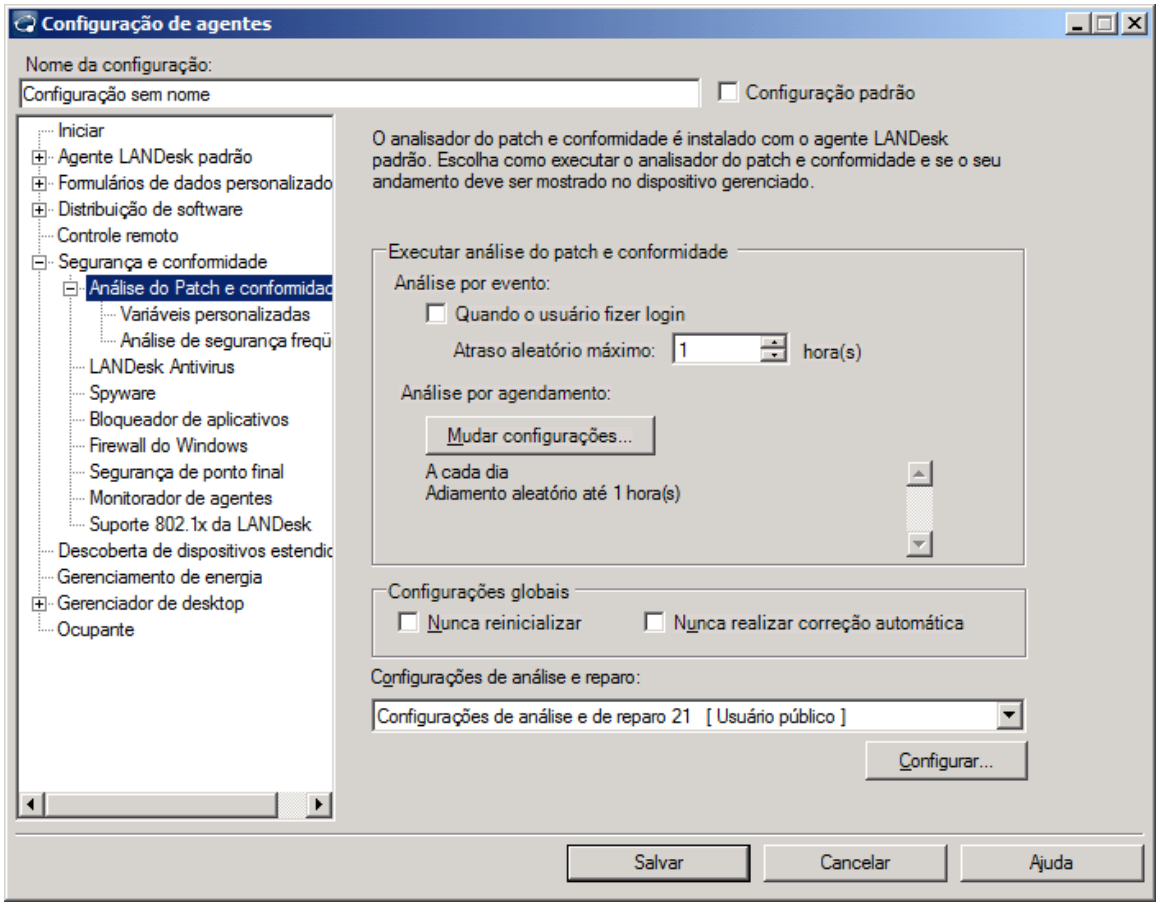
NOTA: A análise dos servidores núcleo e consoles para atualizações de software LANDesk é suportada
É possível analisar também servidores núcleo LANDesk e consoles para as atualizações de software LANDesk, mas eles precisam antes receber a distribuição do agente padrão LANDesk, que inclui o agente do analisador de segurança requerido para as tarefas de análise de segurança.

Configuração de dispositivos Windows para análise de segurança

O agente de análise segurança é incluído como padrão com o agente LANDesk padrão e é instalado em dispositivos tendo a mais básica configuração de agente. Em outras palavras, qualquer dispositivo Windows configurado com a nova ferramenta de Configuração de agente estará pronto para a patch e conformidade.

Configurar dispositivos com a ferramenta Configuração de agente

Use a ferramenta Configuração de agente (**Ferramentas > Configuração > Configuração de agente > Nova configuração do Windows**) para criar configurações de agente com definições de análise de Patch e conformidade especificadas e outras definições de segurança que podem ser distribuídas aos dispositivos alvo.



Para configura dispositivos para análise de segurança e correção através da configuração de agente

1. No console, clique em **Ferramentas > Configuração > Configuração de agentes**.
2. Clique no botão da barra de ferramentas **Novas janelas**.
3. Após especificar os parâmetros desejados para a configuração do agente, clique no grupo **Segurança e conformidade** e, a seguir, clique no **Análise de patch e conformidade**.
4. Selecione o modo como deseja que o analisador de segurança seja executado nos dispositivo gerenciados. Clique em **Ajuda** para obter mais informações sobre uma opção.
5. Selecione uma configuração de análise e reparo na lista disponível para aplicá-la à configuração do agente sendo criado. Você pode criar novas configurações ou editar as configurações existentes clicando em **Configurar**. As configurações de análise e reparo determinam se a varredura de segurança é mostrada em dispositivos durante a execução, as opções de reinicialização, a interação do usuário e os tipos de conteúdo de segurança analisados.
6. Termine de especificar outras definições desejadas para a configuração do agente e clique em **Salvar**.

Ao criar ou editar uma configuração de agente, é possível especificar algumas das opções da análise de segurança, por exemplo, quando e com que freqüência a análise é executada automaticamente nos dispositivos gerenciados, independentemente da análise mostrar o progresso e avisos no dispositivo do usuário final, assim como configurações globais para operações de correção, como, por exemplo, a reinicialização do dispositivo e reparo automático. Para obter mais informações sobre a personalização do comportamento do agente de análise de segurança como parte da criação e distribuição das configurações de agente em dispositivos gerenciados, consulte "Distribuindo serviços de Segurança LANDesk" na página 126.

NOTA: é necessário o WinSock2 em dispositivos Windows 9x para que o agente de análise de segurança seja executado.

Após a configuração terminar, um ícone de programa para o analisador de segurança é adicionado ao grupo de programa **LANDesk Management** no menu **Iniciar** no dispositivo gerenciado. Este programa pode ser usado para executar o analisador diretamente do dispositivo (em vez de ser aberto com aluma chave de execução, início recorrente de agendador local ou tarefa agendada através do console).

Parâmetros adicionais de segurança em configurações de agente

Ao definir uma configuração de agente de dispositivo (para dispositivos Windows), você pode também habilitar e configurar os recursos complementares de segurança como:

- Análise freqüente de segurança para riscos críticos de segurança
- Monitoração de spyware
- Bloqueador de aplicativos
- Firewall do Windows
- Segurança de ponto final que inclui os seguintes componentes: HIPS, LANDesk Firewall e Controle de dispositivo
- Monitorador de agente para monitorar arquivos e serviços
- Suporte para 802.1X NAC que estende o controle de acesso à rede (NAC) com autenticação e conformidade

Consulte as seções abaixo para ver mais informações.

Sobre a página Análise de segurança frequente

Use esta página para habilitar e configurar análises de alta freqüência para riscos de segurança crítica e cronológica como, por exemplo, vírus malignos recém-descobertos e riscos de configuração de firewall.

Essa página contém as seguintes opções:

- **Usar o analisador freqüente de segurança:** Ativa uma análise freqüente de segurança nos dispositivos com essa configuração de agente.
- **Analisar apenas quando houver um usuário conectado:** Restringe a análise de segurança freqüente para que execute somente se um usuário estiver conectado ao dispositivo alvo.
- **A cada:** especifica o intervalo de tempo para uma análise de segurança freqüente.

- **Configurações de análise e reparo (que analisa um grupo):** Especifica as configurações de análise e reparo que controlam o analisador de segurança para análises freqüentes. As configurações de análise e reparo determinam se a análise de segurança são exibidas em dispositivos durante a execução, opções de reinicialização e interação do usuário. A definição selecionada deve ser configurada para analisar um grupo e não um tipo. Se desejar, clique em **Configurar** para criar uma nova configuração de análise e reparo associada a um grupo.

Sobre as páginas Spyware e Bloqueador de aplicativo

Use estas páginas para habilitar e configurar a detecção de spyware e bloqueio de aplicativo em tempo real e sua remoção em dispositivos gerenciados configurados com esta configuração de agente.

IMPORTANTE: Isenção de responsabilidade sobre aplicativo bloqueado
Para ver as informações legais sobre o conteúdo de aplicativo bloqueado, consulte "Isenção de responsabilidades legais para o tipo de aplicativos bloqueados" na página 581.

A detecção de spyware em tempo real verifica somente as definições que residam no grupo de **Análise** e que tiverem a correção automática ligada. Você pode manualmente habilitar a opção de correção automática para definições de spyware carregadas ou configurar atualizações de definição de spyware para que a opção de correção automática seja automaticamente habilitada quando forem carregadas.

A detecção de spyware em tempo real monitora dispositivos para verificar processos iniciados recentemente que tentam modificar o registro local. Se o spyware for detectado, a análise de segurança no dispositivo avisa o usuário final para removê-lo.

Essa página contém as seguintes opções:

- **Permite bloqueamento de spyware em tempo real:** Ativa a monitoração e o bloqueamento de spyware em tempo real nos dispositivos com essa configuração de agente.

  NOTA: Para a análise e detecção de spyware em tempo real funcionar, é necessário habilitar manualmente o recurso de correção automática (autofix) para qualquer definição de spyware descarregada que quiser incluir em uma análise de segurança. As definições de spyware obtidas por download não vêm com o autofix habilitado como padrão.

- **Notificar o usuário quando o spyware for bloqueado:** Exibe uma mensagem que informa o usuário final sobre a detecção e correção de um programa spyware.
- **Se um aplicativo não for reconhecido como spyware, peça aprovação ao usuário antes de ser instalado:** Mesmo se o processo detectado não for reconhecido como spyware de acordo com a lista atual de definições de spyware do dispositivo, o usuário final será avisado antes que o software seja instalado no computador.

Para o bloqueamento de aplicativos em tempo real, a correção NÃO é uma tarefa separada. O bloqueio de aplicativos ocorre como parte da própria análise de segurança, com a edição do registro no disco rígido local para desativar o acesso do usuário aos aplicativos não autorizados. Os serviços de segurança utilizam o programa softmon.exe da ferramenta de monitoração de licença para negar o acesso a executáveis de aplicativos especificados mesmo se o nome de arquivo do executável tiver sido modificado porque o softmon.exe lê as informações do cabeçalho do arquivo.

Essa página contém as seguintes opções:

- **Permitir bloqueamento de aplicativos não autorizados:** Ativa o bloqueamento de aplicativos em tempo real nos dispositivos com essa configuração de agente.
- **Notificar o usuário quando um aplicativo for bloqueado:** Mostra uma mensagem ao usuário final notificando-o que tentaram iniciar um aplicativo não autorizado e o acesso foi negado.

Configurar de dispositivos Linux e UNIX para análise de segurança

O Patch e conformidade suporta também a análise de vulnerabilidade em:

- Red Hat Linux
- SUSE Linux
- Sun Sparc (Solaris 8)

O conteúdo de segurança para cada plataforma pode ser descarregado com o Patch e conformidade como no caso das vulnerabilidades em Windows.

Os dispositivos Linux e UNIX não podem ser configurados com o agente de análise de segurança através da ferramenta de configuração de agente do console. A configuração do dispositivo Linux e UNIX é um processo manual.

Para obter mais informações sobre a instalação dos dispositivos Linux e UNIX, consulte "Configuração de agentes de dispositivos Linux e UNIX" na página 112.

É possível também ver o arquivo README contido no arquivo tar da respectiva plataforma localizado na pasta das plataformas sob ManagementSuite\LDLogon no servidor núcleo.

Uma vez configuradas, pode-se verificar as vulnerabilidades das plataformas Linux e UNIX através das tarefas agendadas do console. Se forem detectadas vulnerabilidades, a correção deve ser feita manualmente no dispositivo afetado.

Configuração de dispositivos Mac OS X para análise de segurança

Nos dispositivos Macintosh OS X, o Patch e conformidade suporta downloads de conteúdo de segurança assim como a análise e correção de segurança.

Além disso, é possível criar e definir a configuração do agente para dispositivos Macintosh com a ferramenta de configuração do Agente. Como no caso da configuração do agente Windows, o agente de análise de segurança é parte do agente padrão da LANDesk para dispositivos Macintosh.

Para obter mais informações sobre como criar e distribuir uma configuração de agente Macintosh com suporte do analisador de segurança, consulte "Gerenciamento de dispositivos Macintosh" na página 480.

Pode-se verificar as vulnerabilidades desses dispositivos Macintosh uma vez configurados, através das tarefas agendadas do console. Se forem detectadas vulnerabilidades, a correção deve ser feita no dispositivo afetado.

Para iniciar manualmente a análise de segurança nos dispositivos Mac

1. Abra **Preferências de sistema** do Mac SO X e selecione a página **LANDesk Client**.
2. Na guia **Visão geral**, clique na seção **Verificar agora** na seção **Segurança**.

Tipos de conteúdo de segurança e assinaturas

Ao instalar o LANDesk Management Suite, a ferramenta Patch e conformidade está agora incluída por padrão (anteriormente, ela era uma adição separada). Entretanto, sem uma assinatura de conteúdo do Security Suite, somente será possível analisar atualizações e definições personalizadas de software LANDesk. Uma assinatura de conteúdo da Security Suite possibilita que você tire total proveito da ferramenta Patch e conformidade ao fornecer acesso a conteúdo adicional de segurança (tipos de definição).

Tipos de conteúdo de segurança do LANDesk Security Suite incluem:

- Atualizações de antivírus (no caso de analisadores de terceiros, inclui somente o conteúdo de detecção do analisador antivírus; no caso do LANDesk Antivirus, inclui o conteúdo de detecção do analisador E os arquivos de definições de vírus)
- Aplicativos bloqueados (consulte "Isenção de responsabilidades legais para o tipo de aplicativos bloqueados" na página 581)
- Definições de vulnerabilidades personalizadas
- Atualizações de drivers
- Atualizações de software LANDesk
- Ameaças à segurança (exposições da configuração do sistema; inclui detecção e configuração de firewall)
- Atualizações de software
- Spyware
- Vulnerabilidades (vulnerabilidades conhecidas específicas de plataforma e aplicativo)

Para obter informações sobre assinaturas de conteúdo, entre em contato com o representante da LANDesk ou visite o site da LANDesk:

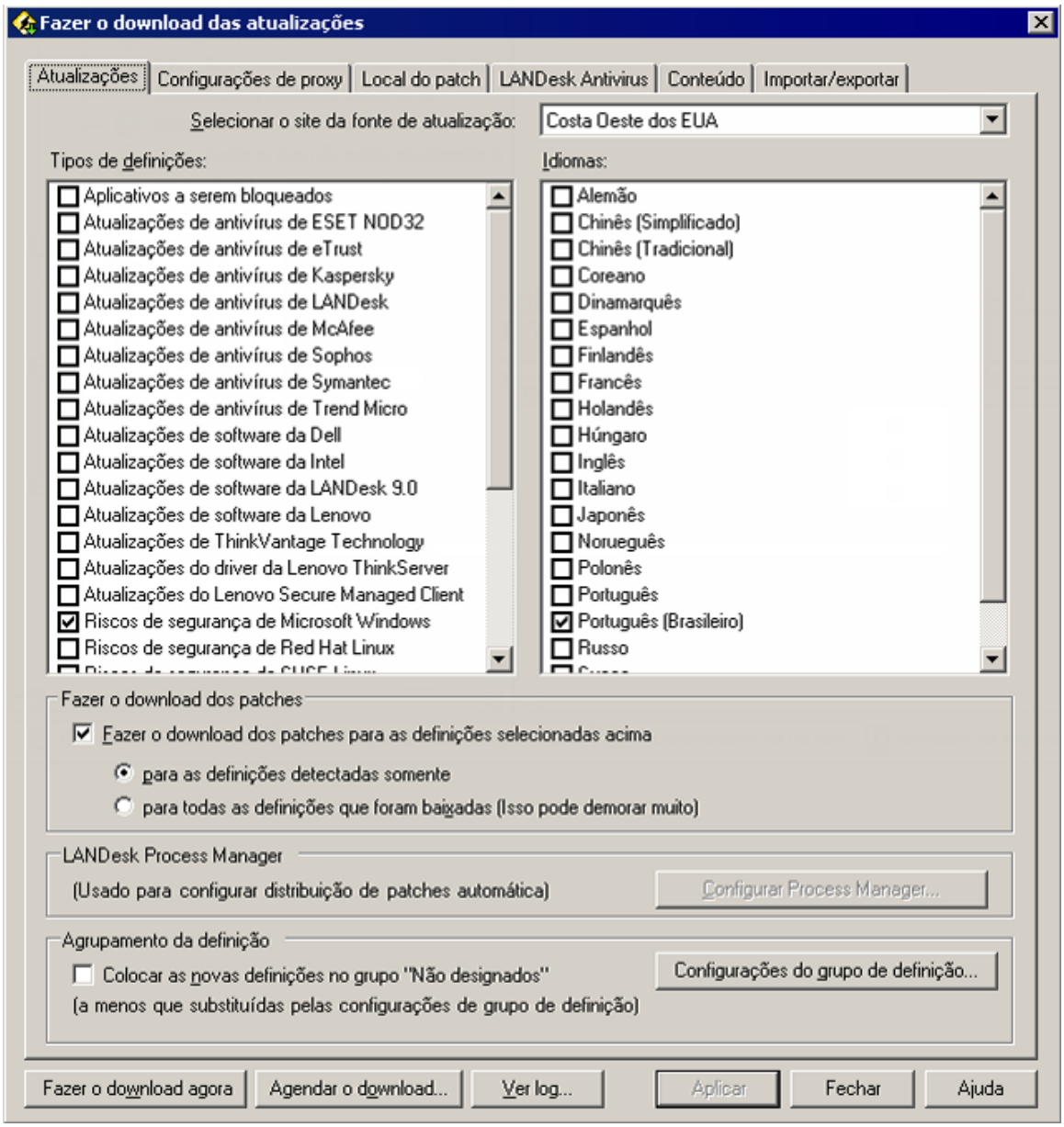
LANDesk Home Page

A Comunidade usuários LANDesk tem fóruns de usuários e os melhores métodos conhecidos para todos os produtos e tecnologia da LANDesk. Para acessar esse recurso valioso, visite:

Página inicial da Comunidade de usuários da LANDesk

Download de atualizações

Observe que a página **Atualizações** da caixa de diálogo **Download de atualizações** inclui várias atualizações de tipos de conteúdo de segurança na lista de tipos de definição.



Funções de análise e correção não são as mesmas entre esses vários tipos de conteúdo. Para obter mais informações sobre como o Patch e conformidade analisa e corrige os tipos diferentes de riscos de segurança detectados em dispositivos gerenciados, consulte as seções apropriadas em "Visão geral de análises de segurança" na página 588.

Tópicos relacionados

"Patch e conformidade" na página 549

"Entenda e use a Janela da ferramenta de Patch e conformidade" na página 555

"Download das atualizações do conteúdo de segurança" na página 571

"Download de patches" na página 579

"Exibir e organizar o conteúdo de segurança." na página 575

"Visão geral de análises de segurança" na página 588

"Visão geral da correção de segurança" na página 598

Download das atualizações do conteúdo de segurança

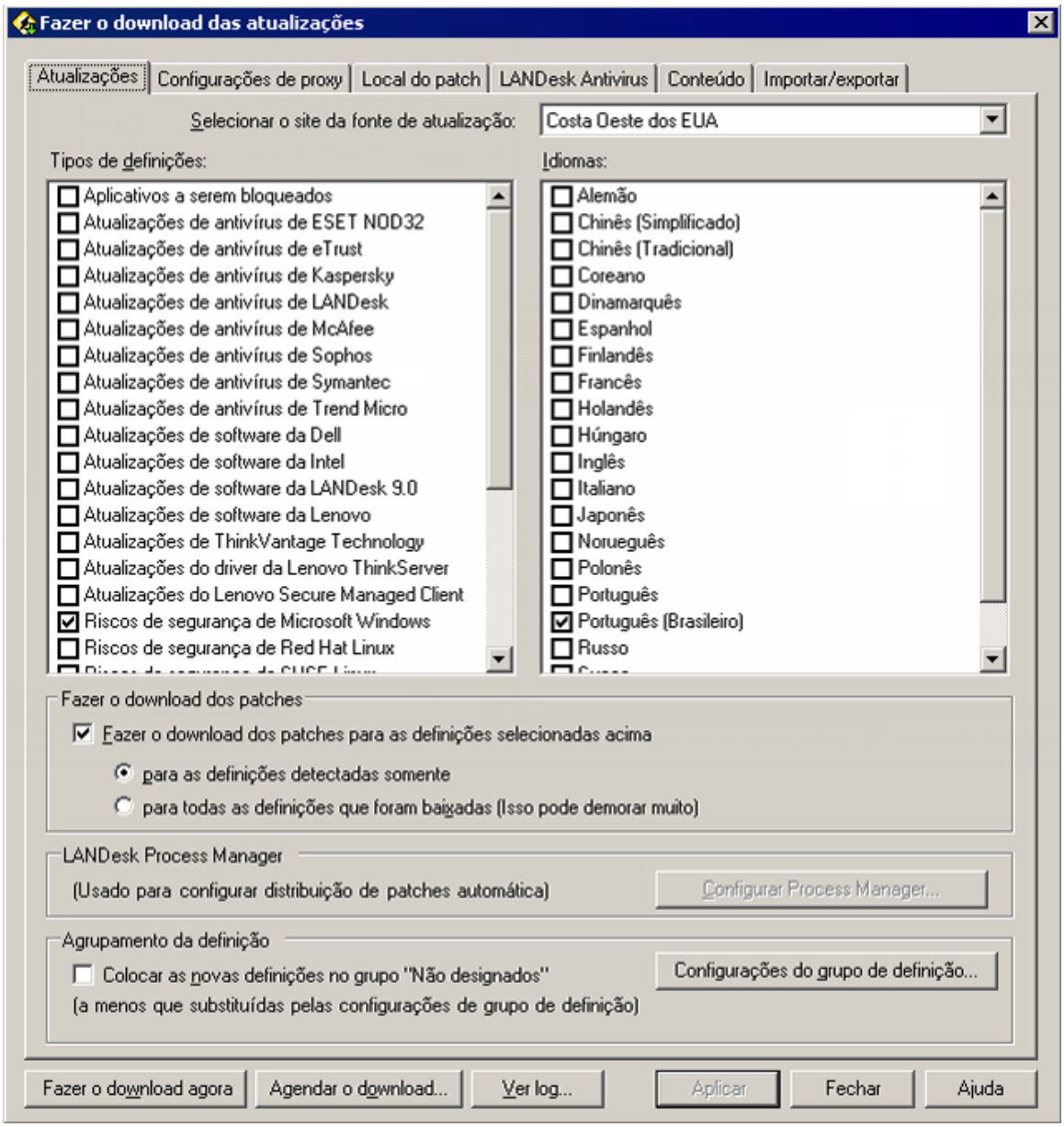
Sua rede e dispositivos estão continuamente vulneráveis a riscos e exposições de segurança de muitas fontes nocivas: worms, vírus, spyware e problemas comuns de manutenção como, atualizações de software e reparos de bugs. Os patches são lançados regularmente para reparar vulnerabilidades inevitáveis do sistema operacional e de aplicativos. A ferramenta Patch e conformidade facilita e acelera o processo de coleta das informações mais recentes sobre definições e patches permitindo o descarregamento de conteúdo por meio de um banco de dados da LANDesk. O serviço LANDesk Security Suite consolida as definições conhecidas de origens confiáveis da indústria/fornecedores e envia as informações confiáveis diretamente a você.

NOTA: O Patch e conformidade também suporta as definições personalizadas de vulnerabilidade Além das vulnerabilidades conhecidas, você também pode criar as suas definições personalizadas de vulnerabilidade e regras associadas de detecção. Para obter mais informações sobre, consulte "Visão geral de definições personalizadas de segurança" na página 581.

Ao estabelecer e manter atualizados os conteúdos de segurança, você pode compreender melhor a natureza e extensão das ameaças contra a segurança para cada plataforma e aplicativo suportados, determinar quais vulnerabilidades e outros tipos de riscos são relevantes ao ambiente e personalizar as tarefas de análise e correção de tarefas. A primeira etapa nesta estratégia de gerenciamento de segurança é descarregar uma lista atual do último conteúdo conhecido de segurança.

Download de atualizações

Use a caixa de diálogo Atualizações de download (clique em **Ferramentas > Segurança > Patch e conformidade > Atualizações de download**) para configurar e fazer atualizações de conteúdo segurança de uma só vez ou criar uma tarefa agendada para ocorrer em um determinado momento ou como uma tarefa recorrente (consulte "Agende atualizações automáticas de conteúdo de segurança" na página 575).



CUIDADO: Somente um usuário LANDesk em um servidor núcleo específico (incluindo consoles adicionais) pode atualizar o conteúdo de segurança em um dado momento. Se um usuário tentar atualizar o conteúdo quando o processo já estiver em execução, aparecerá uma mensagem indicando que há um conflito.

Para descarregar conteúdo de segurança (e patchs)

1. Clique em **Ferramentas > Patch e conformidade**.
2. Clique no botão da barra de ferramentas **Fazer o download das atualizações**.
3. Selecione o site de origem das atualizações na lista de servidores de conteúdo disponíveis.

4. Selecione os tipos de definição cujo conteúdo de segurança que você quer atualizar. Você pode selecionar um ou mais tipos na lista dependendo da sua assinatura de conteúdo da LANDesk Security Suite. Quantos mais tipos você selecionar, maior será o tempo necessário para a atualização.
5. Selecione os idiomas cujo conteúdo você deseja atualizar para os tipos que especificar.

   Alguns tipos de vulnerabilidades e de outras definições, assim como patches associados, têm idioma neutro ou independem do idioma, o que significa que são compatíveis com qualquer versão de idioma do SO ou do aplicativo considerado pela definição. Em outras palavras, não é necessário separar um patch com idioma específico para corrigir essas vulnerabilidades, uma vez que ela abrange todos os idiomas suportados. Por exemplo, as plataformas Linux e UNIX usam somente definições e patches neutros ao idioma. As definições de vulnerabilidade de plataforma do Microsoft Windows e Apple Macintosh, porém, são quase sempre específicas ao idioma.

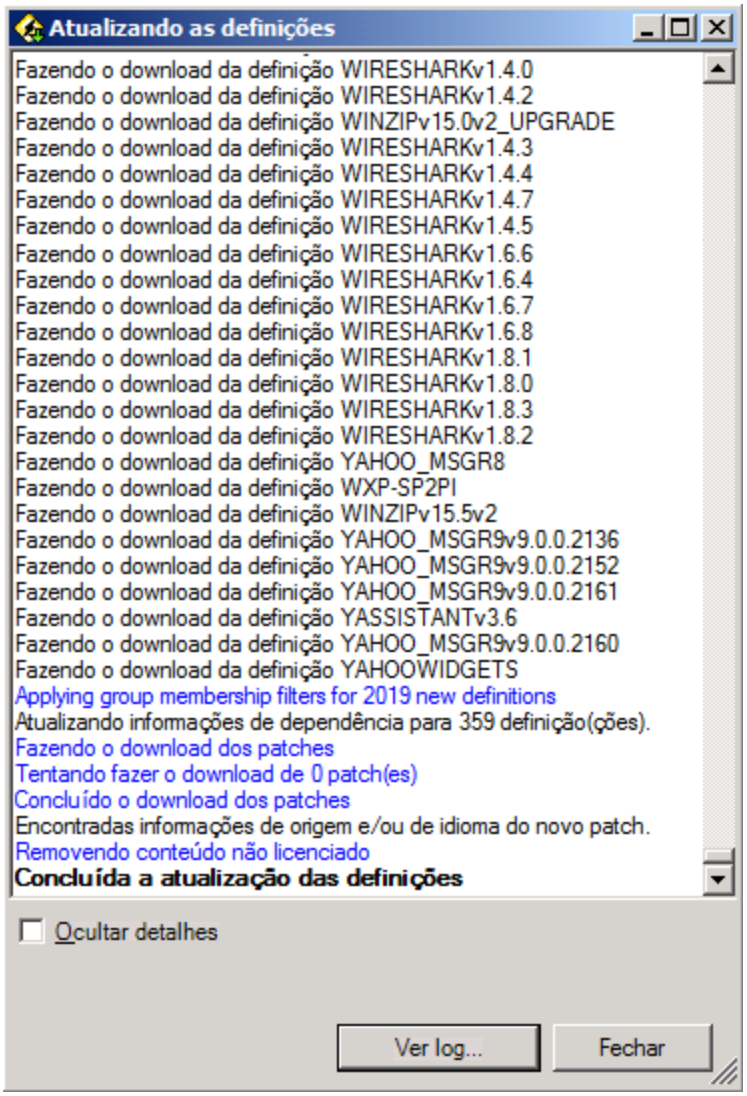
   Ao descarregar o conteúdo de qualquer plataforma (com a assinatura apropriada), todas as definições neutras ao idioma da vulnerabilidade são atualizadas automaticamente, como padrão. Se selecionou o tipo de conteúdo Windows ou Mac, você deverá também selecionar os idiomas específicos cujas definições deseja atualizar. Se selecionou a plataforma Sun Solaris ou Linux, não é necessário selecionar um idioma específico, já que o conteúdo é neutro ao idioma e será atualizado automaticamente.

6. Se você desejar que o novo conteúdo (conteúdo que já não seja residente em nenhum grupo da árvore) seja colocado automaticamente no grupo Não atribuído em vez de no local padrão, que é o grupo Analisar, selecione a caixa de seleção **Colocar as novas definições no grupo "Não designados"**.
7. Se quiser descarregar automaticamente os arquivos executáveis dos patches, selecione na caixa de seleção **Download de patches**, em seguida clique em uma das opções de download. (**NOTA:** Os patches são descarregados no local especificado na página **Local do patch** da caixa de diálogo Download de atualizações.)

   - **Para definições detectadas somente:** Faz download somente dos patches associados às vulnerabilidades, ameaças de segurança ou atualizações da LANDesk detectadas pela última análise de segurança (isto é, as definições que atualmente residem no grupo Detectadas).
   - **Para todas as definições descarregadas:** Descarrega TODOS os patchs associados à vulnerabilidade, ameaças de segurança e atualizações LANDesk atualmente residindo no grupo Analisar.

8. Se tiver um servidor proxy na rede usado para transmissões externas da Internet (necessárias para atualizar o conteúdo de segurança e o download de patches), clique em **Configurações Proxy** e especifique o endereço do servidor, o número da porta e as credenciais de autenticação, se for necessário um login para acessar o servidor proxy.
9. Clique em **Aplicar** a qualquer momento para salvar as configurações.
10. Clique em **Atualizar agora** para executar a atualização de conteúdo de segurança. A caixa de diálogo **Atualização de definições** (veja abaixo) mostra a operação atual e o status. (Para criar uma tarefa agendada, clique em **Agendar atualização**.)

11. Quando a atualização estiver concluída, clique em **Fechar**. Observe que se você clicar em **Cancelar** antes do término da atualização, somente o conteúdo de segurança que já foram processadas até este ponto são inseridas no banco de dados núcleo. Seria necessário executar a atualização novamente para obter o conteúdo de segurança restante.


Atualizando as definições
Fazendo o download da definição WIRESHARKv1.4.0
Fazendo o download da definição WIRESHARKv1.4.2
Fazendo o download da definição WINZIPv15.0v2_UPGRADE
Fazendo o download da definição WIRESHARKv1.4.3
Fazendo o download da definição WIRESHARKv1.4.4
Fazendo o download da definição WIRESHARKv1.4.7
Fazendo o download da definição WIRESHARKv1.4.5
Fazendo o download da definição WIRESHARKv1.6.6
Fazendo o download da definição WIRESHARKv1.6.4
Fazendo o download da definição WIRESHARKv1.6.7
Fazendo o download da definição WIRESHARKv1.6.8
Fazendo o download da definição WIRESHARKv1.8.1
Fazendo o download da definição WIRESHARKv1.8.0
Fazendo o download da definição WIRESHARKv1.8.3
Fazendo o download da definição WIRESHARKv1.8.2
Fazendo o download da definição YAHOO_MSGR8
Fazendo o download da definição WXP-SP2PI
Fazendo o download da definição WINZIPv15.5v2
Fazendo o download da definição YAHOO_MSGR9v9.0.0.2136
Fazendo o download da definição YAHOO_MSGR9v9.0.0.2152
Fazendo o download da definição YAHOO_MSGR9v9.0.0.2161
Fazendo o download da definição YASSISTANTv3.6
Fazendo o download da definição YAHOO_MSGR9v9.0.0.2160
Fazendo o download da definição YAHOOWIDGETS
Applying group membership filters for 2019 new definitions
Atualizando informações de dependência para 359 definição(ções).
Fazendo o download dos patches
Tentando fazer o download de 0 patch(es)
Concluído o download dos patches
Encontradas informações de origem e/ou de idioma do novo patch.
Removendo conteúdo não licenciado
Concluída a atualização das definições
Ocultar detalhes
Ver log...
Fechar

CUIDADO: Não encerre o console durante a atualização manual
Não encerre o console durante um processo manual de atualização de conteúdo de segurançaou o processo será encerrado. Esta regra, porém, não se aplica à tarefa agendada, que terminará de processar mesmo se o console estiver fechado durante a execução.

Para configurar o local de download dos patches

1. Na caixa de diálogo **Atualização de downloads**, clique na guia **Local do patch**.
2. Digite um caminho UNC para onde os arquivos de patches serão copiados. O local padrão é o diretório \LDLogon\Patch do servidor núcleo.

3. Se o caminho UNC digitado for de um local diferente do servidor núcleo, digite um nome de usuário e uma senha válidos para autenticar-se nesse local.
4. Digite um URL da Web onde os dispositivos possam acessar os patches descarregados por download para distribuição. Este URL da Web deve ser igual ao caminho UNC acima.
5. Você pode clicar em **Testar configurações** para verificar se uma conexão com o endereço da Web especificado acima pode ser feita.
6. Se desejar restaurar o caminho UNC e o URL da Web para um dos locais padrão, clique em **Restaurar para o padrão**. Repetimos, local padrão de armazenamento é o diretório \LDLogon\Patch do servidor núcleo.

Agende atualizações automáticas de conteúdo de segurança

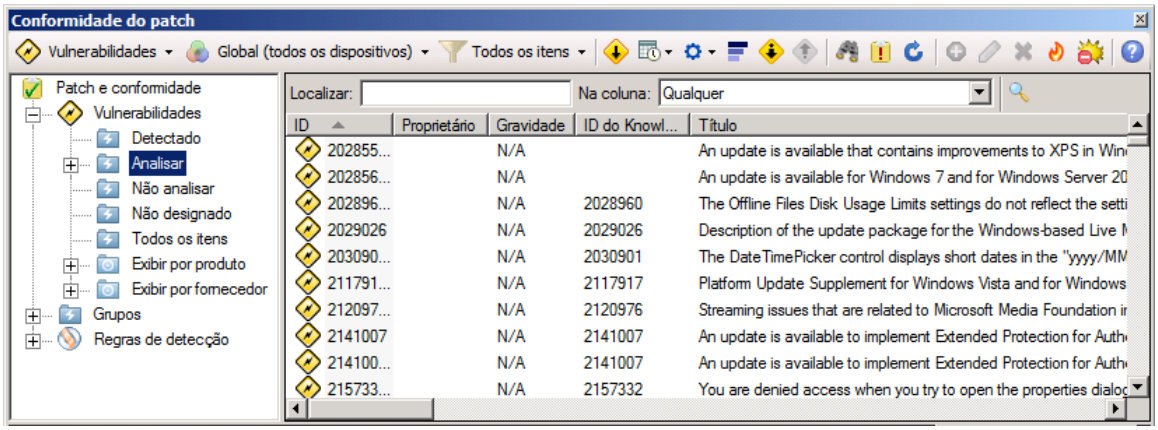
Também é possível configurar as atualizações de conteúdo de segurança como uma tarefa agendada a ser realizada em um determinado horário como tarefa recorrente. Para isso, clique no botão **Agendar download** na barra de ferramentas. A caixa de diálogo **Informações de atualização agendada** mostra configurações específicas à tarefa. Clique em **OK** para criar uma tarefa de Download de Conteúdo de Segurança na janela Tarefas agendadas, onde você pode especificar as opções de agendamento.

IMPORTANTE: Configurações de tarefas e específicas globais
Observe que somente os tipos de definição, idiomas e configurações de download de definição e patch são salvos e associados a uma tarefa específica ao criá-la. Essas três definições são consideradas específicas a tarefas. Entretanto, todas as definições nas outras páginas da caixa do diálogo **Download de atualizações** são globais, o que significa que se aplicam a todas as tarefas subsequentes de download de conteúdo de segurança. As configurações globais incluem o local de download do patch, servidor proxy, correção automática de spyware, alertas de segurança e antivírus. Quando você mudar as configurações globais, elas estarão em efeito para todas as tarefas de download de conteúdo de segurança daquele momento em diante.

Exibir e organizar o conteúdo de segurança.

Depois que o conteúdo de segurança tiver sido atualizado, você pode ver as definições e regras de detecção (somente para vulnerabilidades e definições personalizadas) nos respectivos grupos da janela da ferramenta do Patch e conformidade.

Use a lista suspensa **Tipo** para ver o conteúdo de um tipo específico de definição ou para todos os tipos. Você também pode usar o controle **Filtro** para personalizar ainda mais o conteúdo que quiser mostrar.



Quando o conteúdo de segurança tiver sido descarregado, você pode mover os itens em grupos diferentes de status ou copiá-los nos respectivos grupos personalizados. Para obter mais informações sobre como usar os grupos diferentes, consulte "Entenda e use a Janela da ferramenta de Patch e conformidade" na página 555.

Você também pode mostrar os detalhes de propriedade para cada uma das definições e regras de detecção atualizadas clicando com o botão direito em um item e selecionando **Propriedades**. Essas informações podem ajudá-lo a determinar quais definições são relevantes para as plataformas e os aplicativos suportados na rede, como as regras de detecção verificam a presença de definições, quais patches estão disponíveis e como quer configurar e realizar correções nos dispositivos afetados.

NOTA: As definições personalizadas podem ser modificadas
Se você selecionou uma definição descarregada da indústria, a caixa de diálogo de propriedades é destinado apenas para informações. No entanto, se você selecionar uma definição personalizada ou estiver criando uma nova definição personalizada, as páginas e os campos da caixa de diálogo de propriedades são editáveis, permitindo que você escolha a definição e suas regras de detecção.

Procurar vulnerabilidades por nomes CVE

Patch e Conformidade suporta a convenção de nomes CVE (Common Vulnerabilities and Exposures). Você pode pesquisar por uma vulnerabilidade baixada pelo seu nome CVE. Você também pode exibir o(s) nome(s) CVE associado(s) à uma vulnerabilidade individual.

O que é CVE?

CVE (Common Vulnerabilities and Exposures) é uma iniciativa colaborativa de várias organizações líderes de tecnologia de segurança para compilar e manter uma lista de nomes padronizados para vulnerabilidades e outras exposições de segurança de informação. CVE é um dicionário de nomes e não um banco de dados.

Em resumo, o objetivo declarado da convenção de nomes CVE é o de tornar mais fácil a procura, o acesso e o compartilhamento de dados entre banco de dados de vulnerabilidades e ferramentas de segurança. Para encontrar mais detalhes sobre CVE e o Conselho Editorial da CVE, visite o site da MITRE Corporation.

Compatibilidade LANDesk com a convenção de nomes CVE

Os produtos da LANDesk, inclusive o produto principal do LANDesk Management Suite assim como o LANDesk Security Suite e o LANDesk Patch Manager, oferecem ferramentas para a atualização de definições de vulnerabilidade, exibição e relatório que suportam totalmente o padrão CVE.

Ao fazer o download de atualizações de definição de vulnerabilidade, os dados de vulnerabilidade contêm referências de nome CVE baseados nas informações mais recentes da junta CVE. Além disso, a definição de vulnerabilidade inclui um hyperlink ao site de dicionário CVE onde residem as mais recentes informações da versão CVE na origem. A precisão e atualização dos dados CVE são validados por esse link direto.

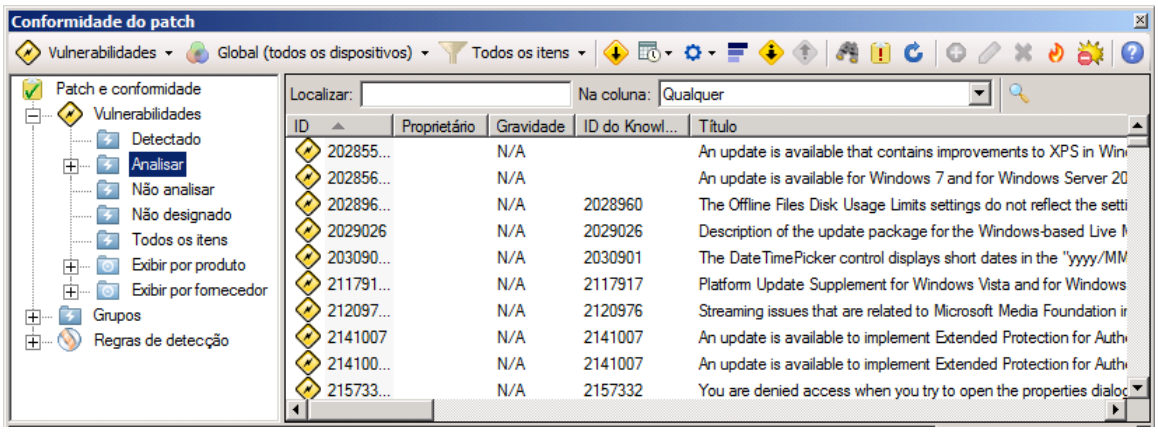
Procurar vulnerabilidades por seus nomes CVE

O Patch e Conformidade permite a procura de vulnerabilidades pelos nomes CVE exclusivos.

Você também encontra nomes CVE para vulnerabilidades descarregadas assim como o acesso ao site CVE para ver mais informações sobre a vulnerabilidade e seu status CVE.

Para encontrar definições de vulnerabilidade de segurança usando os nomes CVE

1. No **Patch e Conformidade**, selecione **Vulnerabilidades** na lista suspensa **Tipo**. Aparecerá uma lista completa das definições de vulnerabilidades descarregadas.


Conformidade do patch
Vulnerabilidades
Global (todos os dispositivos)
Todos os itens
Patch e conformidade
Vulnerabilidades
Detectado
Analisar
Não analisar
Não designado
Todos os itens
Exibir por produto
Exibir por fornecedor
Grupos
Regras de detecção
Localizar:
Na coluna:
Qualquer
ID
Proprietário
Gravidade
ID do Knowl...
Título
202855... N/A An update is available that contains improvements to XPS in Win
202856... N/A An update is available for Windows 7 and for Windows Server 20
202896... N/A 2028960 The Offline Files Disk Usage Limits settings do not reflect the setti
2029026 N/A 2029026 Description of the update package for the Windows-based Live
203090... N/A 2030901 The DateTimePicker control displays short dates in the "yyyy/MM
211791... N/A 2117917 Platform Update Supplement for Windows Vista and for Windows
212097... N/A 2120976 Streaming issues that are related to Microsoft Media Foundation i
2141007 N/A 2141007 An update is available to implement Extended Protection for Auth
214100... N/A 2141007 An update is available to implement Extended Protection for Auth
215733... N/A 2157332 You are denied access when you try to open the properties dialo

2. Digite o nome CVE (ID CVE) no campo **Localizar**, selecione **Qualquer** ou **ID CVE** na lista **Na coluna** e clique no botão **Pesquisar**. (É possível digitar o ID CVE inteiro, inclusive o prefixo cve-, ou toda a parte do ID que souber, e procurar no repositório de segurança descarregado as vulnerabildiades correspondentes.)
3. Se uma vulnerabilidade com ID CVE correspondente for encontrada no repositório de vulnerabilidades descarregadas com o Patch e Conformidade, ela será mostrada na lista.
4. Clique com o botão direito na vulnerabilidade para acessar o menu de atalho e ver as opções disponíveis.

Para encontrar nomes CVE para definições descarregadas de vulnerabilidade de segurança

1. Em **Patch e Conformidade**, selecione **Vulnerabilidades** ou **Todos os tipos** na lista **Tipo**. Aparecerá uma lista das definições descarregadas. (Se a coluna dos dados ID CVE foi selecionada, você poderá ver os ID CVE na lista de itens. Para configurar colunas, clique com o botão direito na barra de títulos da coluna, selecione **Colunas** e verifique se a coluna **ID CVE** está na lista **Colunas selecionadas**.)
2. Clique duas vezes na definição de vulnerabilidade (ou clique duas vezes na definição e selecione **Propriedades**) para abrir a caixa de diálogo **Propriedades**.
3. Clique na página **Descrição**.
4. Se a vulnerabilidade selecionada tiver um nome CVE, ele aparece na lista **ID CVE**. Algumas vulnerabilidades podem ter mais do que um nome CVE e você poderá acessá-lo(s) na lista.
5. Para acessar a página de um ID CVE específico, clique no link **Mais informações para o ID CVE**. O site da CVE fornece informações detalhadas sobre cada vulnerabilidade com nome CVE, inclusive o status atual na junta CVE (Entrada aprovada ou Candidato sob revisão).

Personalizar listas de itens com filtros

A lista **Filtro** permite a criação e aplicação de filtros de exibição personalizados para controlar os itens mostrados no quadro do lado direito da janela da ferramenta. Os filtros podem ajudar a dinamizar uma grande quantidade de conteúdo de segurança. Você pode filtrar o conteúdo por sistema operacional e gravidade.

O controle **Filtro** pode ser usado em conjunto com o controle **Tipo** para mostrar exatamente o conteúdo de segurança no qual estiver interessado.

Para criar um novo filtro de exibição

1. No Patch e conformidade, clique na lista suspensa **Filtro**, em seguida clique em **Gerenciar filtros**.
2. Clique em **Nova**.
3. Digite um nome para o novo filtro.
4. Se quiser filtrar por sistema operacional, selecione a caixa de seleção **Sistema Operacional**e, em seguida, selecione os sistemas operacionais que quiser mostrar.
5. Se quiser filtrar por gravidade da definição, marque a caixa de seleção **Severidade** e em seguida, selecione as gravidades que quiser exibir. Clique em **OK**.

Para aplicar um filtro a uma tela de grupo de conteúdo

1. Clique no grupo do conteúdo no painel esquerdo da janela.
2. Clique na lista suspensa **Filtro**, em seguida selecione um filtro na lista.

Eliminar definições conteúdo de segurança.

Você pode excluir as definições não usadas da janela do Patch e conformidade e do banco de dados núcleo se decidir que elas não são relevantes para seu ambiente ou se uma correção bem-sucedida as torna obsoletas.

Quando você exclui definições, as informações da regra de detecção associadas também são removidas dos grupos Regras de detecção da exibição em árvore. Entretanto, os arquivos reais associados do patch não são removidos por este processo. Os arquivos dos patches devem ser removidos manualmente do repositório local, que normalmente se encontra no servidor núcleo.

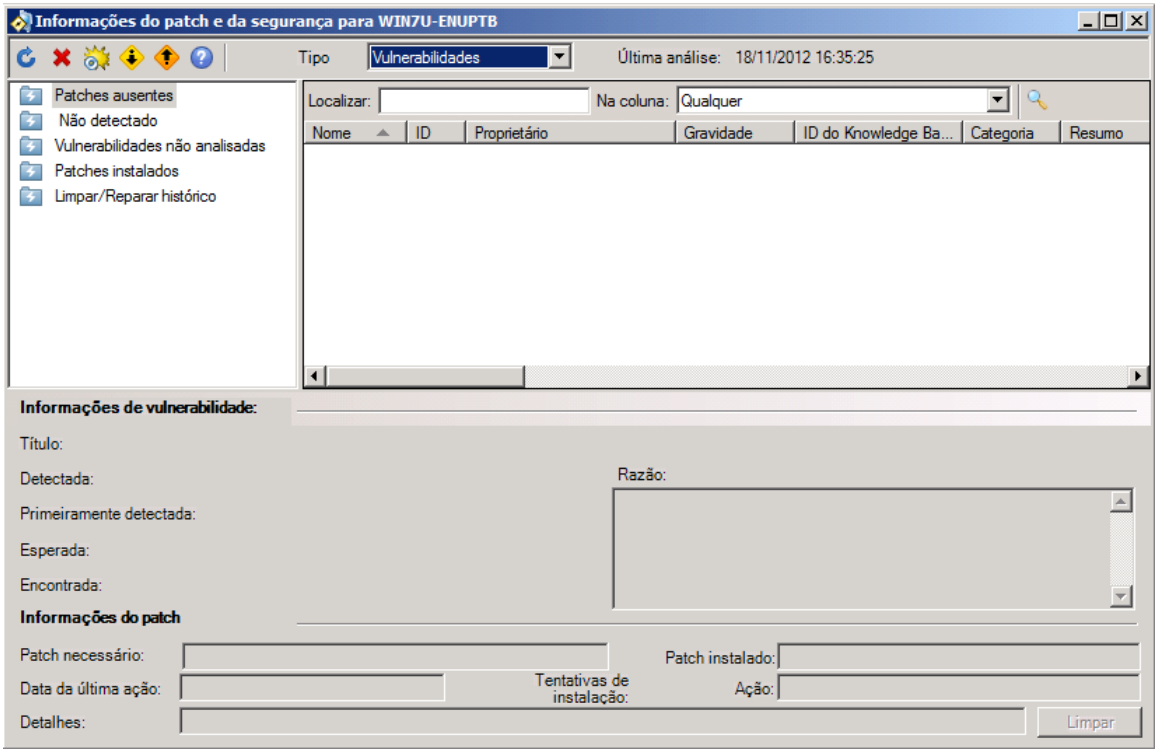
Para excluir definições não usadas

1. Clique em **Ferramentas > Patch e conformidade**.
2. Clique no botão da barra de ferramentas **Purgar definições não utilizadas**.
3. Selecione as plataformas cujas definições você quer remover. Selecione uma ou mais plataformas na lista. Se uma definição estiver associada a mais de uma plataforma, você deverá selecionar todas as suas plataformas associadas para que a definição seja removida.
4. Selecione os idiomas cuja definição você quer remover (associadas à plataforma selecionada acima). Se você selecionar uma plataforma Windows ou Macintosh acima, deverá especificar os idiomas cuja definição quer remover. Se selecionar uma plataforma UNIX ou Linux acima, deverá selecionar a opção Independente de idioma para remover as definições independentes de idioma.
5. Clique em **Remover**.

Exibir informações de segurança de um dispositivo analisado

Você também pode exibir as informações específicas de um dispositivo analisado diretamente da tela de rede clicando com o botão direito em um ou mais dispositivos selecionados e, em seguida, clicando em **Informações de segurança e patch**.

Essa caixa de diálogo permite a exibição de detecção, instalação e histórico de reparos e realizar tarefas de gerenciamento de patch.



Download de patches

Para distribuir patches de segurança para dispositivos afetados, o arquivo executável de correções deve primeiro ser descarregado por download em um repositório local de patches na rede. O local padrão para downloads de arquivos de patches é o diretório no servidor núcleo.

/LDLogon/Patches

Você pode mudar esse local na página Local do patch da caixa de diálogo Download.

Você pode fazer o download de um patch de cada vez ou de um conjunto de patches juntos.

NOTA: Configurações do local de download de patch e do servidor proxy
Os downloads de patches sempre usam as configurações do local de download atualmente presentes na página Local do patch da caixa de diálogo Download de atualizações. Observe também que, se a rede usar um servidor proxy para acesso à Internet, você deverá primeiro definir as configurações do servidor proxy na página Configurações Proxy antes de fazer o download de arquivos patch.

O Patch e conformidade tenta primeiro fazer o download de um arquivo de correções a partir do URL (exibido na caixa de diálogo Propriedades de correção). Se não for possível fazer uma conexão, ou se o patch não estiver disponível por alguma razão, o patch é descarregado do serviço de segurança da LANDesk, que é um banco de dados da LANDesk contendo patches de fontes confiáveis da indústria.

Métodos de download

Use um dos seguintes métodos para descarregar patches:

- A partir da caixa de diálogo Download de atualizações
- Da regra de detecção

- Da definição de segurança

Você pode fazer o download de patches da caixa de diálogo Download de atualizações simultaneamente com suas definições de segurança associadas.

Você pode também descarregar patchs diretamente de uma regra de detecção ou de uma definição de segurança.

Para descarregar patchs de uma regra de detecção

1. De qualquer grupo **Regras de detecção**, clique com o botão direito em uma regra de detecção e, em seguida, clique em **Download de patch**. (O download dos patches para as definições personalizadas também pode ser feito a partir da caixa de diálogo Regra de detecção ao criar ou editar uma definição personalizada.)
2. Para fazer o download de um conjunto de correções, selecione qualquer número de regras em qualquer grupo **Regras de detecção**, clique o botão direito na seleção e, em seguida, clique em **Download patch**.
3. A operação de download e o status são exibidos na caixa de diálogo **Fazendo o download dos patches**. Você pode clicar em **Cancelar** a qualquer momento para interromper o processo de download.
4. Quando o download estiver concluído, clique no botão **Fechar**.

NOTA: Com uma regra de detecção, você também pode fazer o download de patches a partir da caixa de diálogo propriedades (**Propriedades > Informações de patch > Download**)

Para descarregar patches associados de uma definição de segurança

1. Clique com o botão direito na definição de segurança, clique em **Fazer o download de patches associados**.
2. Selecione se que descarregar todos os patches associados ou apenas os atuais.
3. Clique em **Download**.

Para obter mais informações sobre o status de download do arquivo de patch, consulte "Entenda e use a Janela da ferramenta de Patch e conformidade" na página 555.

Desinstalar patches (reverter patch)

Você pode também desinstalar (isto é, reverter) patches que tenham sido distribuídos em dispositivos gerenciados. Por exemplo, você pode decidir desinstalar um patch que tenha causado um conflito inesperado com uma configuração existente. Ao desinstalar o patch, você pode restaurar o dispositivo ao seu estado original.

Para desinstalar ou reverter um patch

1. De qualquer lista de regra de detecção, clique com o botão direito em uma ou mais regras, em seguida clique em **Desinstalar patch**.
2. Digite um nome para a tarefa de remoção.
3. Especifique se a desinstalação é uma tarefa agendada ou uma análise baseada em diretivas, ou ambas.
4. Se você selecionou tarefa agendada, especifique os dispositivos quer desinstalar o patch.

5. Se o patch não puder ser desinstalado sem acessar o seu arquivo executável original (por exemplo, para usar parâmetros de linha de comando) e você quiser distribuir o executável usando a Multidifusão dirigida, marque a caixa de seleção **Usar multidifusão**. Para configurar as opções de Multidifusão, clique no botão **Opções de multidifusão**. Para obter mais informações, consulte "Sobre a caixa de diálogo Opções de multidifusão" na página 640.
6. Se selecionou diretiva e quiser criar uma nova pesquisa baseada nesta tarefa de desinstalação que pode ser usada mais tarde, clique na caixa de seleção **Acrescentar uma consulta**.
7. Selecione configurações de análise e reparo na lista disponível (ou crie configurações personalizada dessa análise) para determinar como a análise funciona nos dispositivos do usuário final.
8. Clique em **OK**. Para uma tarefa agendada, agora você pode acrescentar dispositivos de origem e configurar as opções de agendamento na ferramenta Tarefas agendadas. Para uma diretiva, a nova diretiva aparece na janela do Application Policy Management com o nome de tarefa especificado acima. Nessa tela você pode adicionar alvos estáticos (usuários ou dispositivos) e alvos dinâmicos (resultados de consultas) e configurar o tipo e a freqüência da diretiva.

Se houver uma falha na instalação de uma correção, você deverá primeiro limpar essas informações de status antes de tentar instalar novamente a correção. Você pode limpar o status da instalação (reparar) do dispositivo selecionado clicando em **Limpar**, na caixa de diálogo **Informações de segurança e patch**. Você também pode limpar o status de instalação do patch por vulnerabilidade.

Remover patches do banco de dados núcleo

Para remover arquivos de patches permanentemente, você deve excluí-los do repositório de patches, que normalmente se encontra no servidor núcleo.

Isenção de responsabilidades legais para o tipo de aplicativos bloqueados

IMPORTANTE: A LANDesk fornece acesso aos seus usuários finais a um banco de dados com determinadas informações sobre arquivos executáveis que um usuário final pode usar em conexão com a funcionalidade bloqueadora de aplicativo do LANDesk Security Suite. ESTAS INFORMAÇÕES SÃO FORNECIDAS NO ESTADO EM QUE SE ENCONTRAM, SEM NENHUMA GARANTIA EXPRESSA, IMPLÍCITA OU DE QUALQUER TIPO, INCLUINDO MAS NÃO LIMITADO ÀS GARANTIAS IMPLÍCITAS DE COMERCIABILIDADE E/OU ADEQUAÇÃO A UM PROPÓSITO EM PARTICULAR. Como tal, a LANDesk não garante a precisão, integridade ou a atualidade dessas informações e o usuário final é responsável pela leitura/entendimento e confirmação dessas informações antes do uso. Os usuários finais utilizarão essas informações a seu próprio risco.

Algumas das informações do Resumo presente nas definições de aplicativos bloqueados são fornecidas a partir de: http://www.sysinfo.org, e é Protegido por Direitos Autorais, da seguinte forma: "Apresentações, formato e comentários Copyright © 2001-2005 Paul Collins; Partes do Copyright © Peter Forrest, Denny Denham, Sylvain Prevost, Tony Klein; Criação e suporte do banco de dados por Patrick Kolla; Suporte de software por John Mayer; Todos os direitos reservados."

Visão geral de definições personalizadas de segurança

Além das vulnerabilidades conhecidas atualizadas através da ferramenta Patch e conformidade, você também pode criar suas definições personalizadas (ou definidas pelo usuário), completas com as regras de detecção personalizadas, arquivos patch associados e comandos adicionais especiais para assegurar uma correção bem sucedida.

As definições de vulnerabilidade consistem em um ID único, título, data de publicação, idioma e outras informações de identificação assim como regras de detecção que informam a análise de segurança sobre o que verificar nos dispositivos de destino. As regras de detecção definem a plataforma específica, o aplicativo, o arquivo ou as condições de registro que a análise de segurança verifica a fim de detectar uma vulnerabilidade (ou praticamente any condição ou status do sistema) em dispositivos analisados.

As definições personalizadas de vulnerabilidade constituem um recurso potente e flexível que permite a implementação de um nível adicional proprietário de segurança de patch no sistema LANDesk. Além de melhorar a segurança da correção, as vulnerabilidade personalizadas podem ser usadas para acessar configurações do sistema, verificar configurações específicas de arquivo e registro e distribuir atualizações, entre outros usos inovadores que aproveitam as vantagens da capacidade de análise da varredura de vulnerabilidade.

NOTA: Criação de definições de aplicativos bloqueados
Crie também suas próprias definições do tipo de aplicativo bloqueado. Na lista suspensa **Tipo**, selecione **Aplicativos bloqueados**, digite um nome de arquivo para o executável e um título descritivo para a definição, em seguida, clique **OK**.

As definições personalizadas não precisam executar ações de correção (distribuição e instalação de arquivos patch). Se a definição personalizada estiver definida com a regra de detecção Somente detectar que só pode ser detectada pelo Patch e conformidade, a análise de segurança verifica os dispositivos alvo e simplesmente reporta os dispositivos onde a condição prescrita da regra (por exemplo, vulnerabilidade é encontrada). Por exemplo, você pode gravar uma regra personalizada Somente detectar para que a análise de segurança verifique os dispositivos gerenciados dos itens a seguir:

- Existência de aplicativo
- Existência de arquivo
- Versão do arquivo
- Local do arquivo
- Data do arquivo
- Configuração do registro

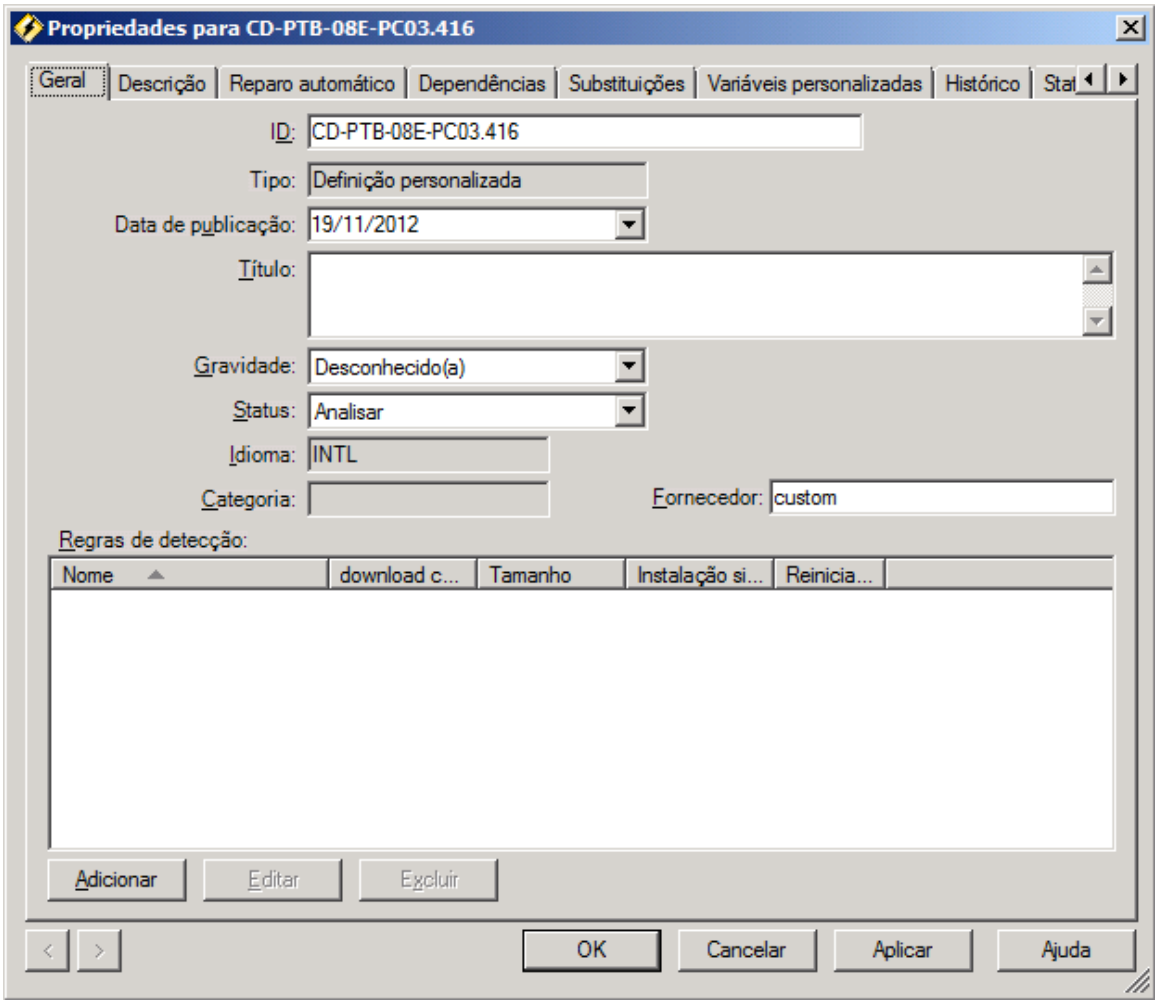
Você pode criar todas as definições de vulnerabilidade necessárias para estabelecer e manter o nível ótimo de segurança de patch no seu ambiente.

Criar definições personalizadas de vulnerabilidade

Para criar definições personalizadas

1. Clique em **Ferramentas > Patch e conformidade**.
2. Na lista **Tipo**, selecione **Todos os tipos** ou **Definições personalizadas**.. (O botão **Criar definição personalizada** da barra de ferramentas fica disponível somente com um desses dois tipos selecionados ou com o tipo de **Aplicativos bloqueados** selecionado, se quiser criar uma definição personalizada de aplicativo bloqueado.)

3. Clique no botão **Criar definição personalizada** da barra de ferramentas. Uma versão editável da caixa de diálogo propriedades é exibida, permitindo as configurações das definições de vulnerabilidade.



4. Digite um ID exclusivo para a vulnerabilidade. (O código de ID gerado pelo sistema é editável.)
5. O tipo é uma Definição personalizada e não pode ser modificada.
6. A data de publicação é o dia de hoje e não é editável.
7. Digite um título descritivo para a vulnerabilidade. Este título é exibido em listas de vulnerabilidade.
8. Especifica o nível de severidade. As opções disponíveis são: Desconhecido, Service Pack, Crítico, Alto, Médio, Baixo e Não aplicável.
9. Especifica o status da vulnerabilidade. As opções disponíveis são: Não analisar, Analisar e Não atribuída. Ao especificar um status, a vulnerabilidade é colocada no grupo correspondente na tela de árvore (consulte "Tela da árvore" na página 558).

10. As configurações de idioma para as vulnerabilidades definidas pelo usuário são feitas automaticamente para o INTL (Internacional ou independente de idioma, significando que a vulnerabilidade pode ser aplicada a qualquer versão de idioma dos sistemas operacionais e/ou aplicativos).
11. A lista Regras de detecção mostra todas as regras usadas por esta vulnerabilidade. Se estiver criando uma nova vulnerabilidade personalizada, configure pelo menos uma regra de detecção que é usada pela análise de segurança para analisar dispositivos para a vulnerabilidade. Para acrescentar regras de detecção, clique em **Adicionar**. (Consulte o procedimento a seguir para obter as instruções detalhadas.)
12. Se quiser oferecer informações adicionais sobre esta vulnerabilidade, clique em **Descrição** e digite os seus comentários no quadro de texto e/ou insira um endereço de Web válido onde residem as informações adicionais.
13. Se você quer incluir prerrequisitos para esta definição personalizada de vulnerabilidade (e exibir todas as outras definições dependentes nesta vulnerabilidade), clique em **Dependências** e configure as definições de prerrequisito.
14. Se você quiser criar (ou editar) suas próprias variáveis personalizadas para esta definição personalizada, clique em **Variáveis personalizadas** e configure as variáveis personalizadas.
15. Quando você é feitos especificar atributos para a vulnerabilidade personalizada, clique em **OK** para fechar a caixa de diálogo e salvar a definição de vulnerabilidade.

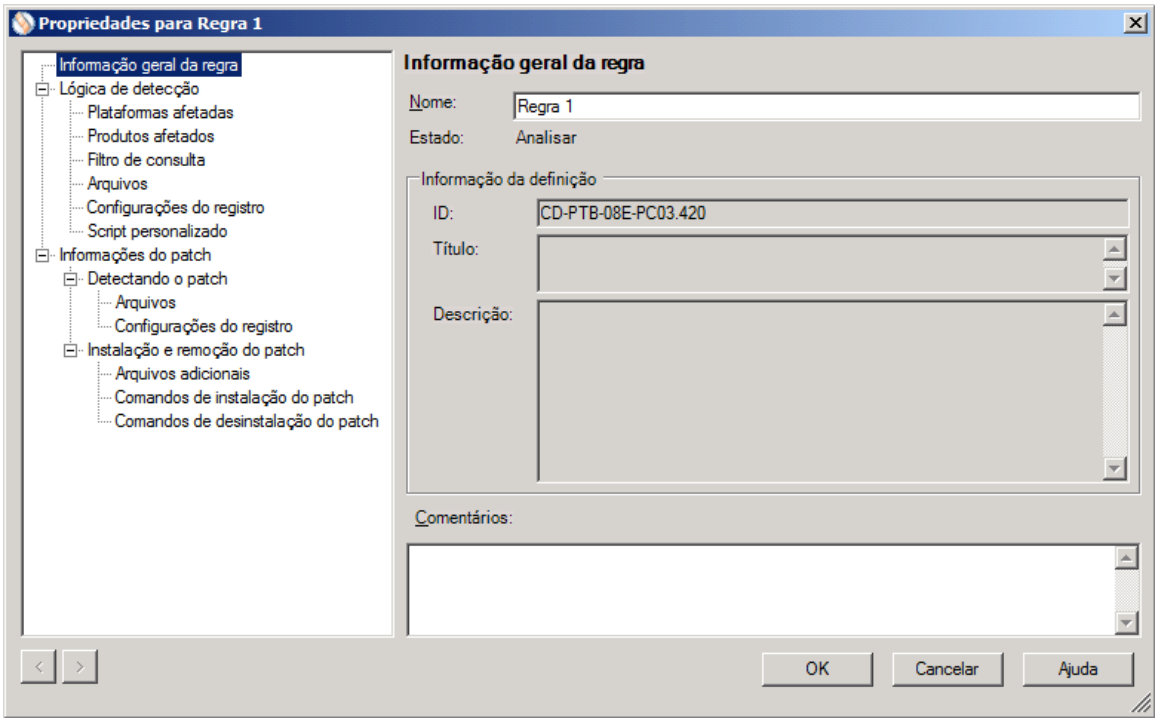
Como nas vulnerabilidades conhecidas de fornecedores, as vulnerabilidades personalizadas devem incluir uma ou mais regras de detecção que informam à análise de segurança quais condições observar durante a análise de dispositivos gerenciados. Siga os passos a seguir para criar uma regra de detecção para uma vulnerabilidade personalizada.

Criação de regras personalizadas de detecção

Para criar regras personalizadas de detecção

1. Clique com o botão direito numa definição personalizada, em seguida, clique em **Propriedades**. (Ou clique duas vezes na definição da vulnerabilidade).

2. Clique no botão **Adicionar** sob a lista Regras de detecção. Uma versão editável da caixa de diálogo Propriedades de regras é aberta na página de Informações gerais da caixa de diálogo, permitindo a configuração de uma regra de detecção.



3. Na página de Informações gerais, insira um nome único para a regra. O status da regra não pode ser modificado aqui. Para mudar o status de uma regra de detecção, clique com o botão direito na regra em qualquer lista, em seguida clique em **Habilitar** ou **Desabilitar**, dependendo do estado atual. As informações de definição da regra não podem ser modificadas aqui, tampouco. Todavia, você pode inserir quaisquer informações que quiser no quadro Comentários.
4. Use as várias páginas da caixa de diálogo Propriedades das regras para definir a regra de detecção, conforme descrito no restante deste procedimento.
5. Abra as páginas Lógica de detecção.
6. Na página Plataformas afetadas, selecione as plataformas nas quais executar a análise de segurança para verificar esta definição da regra de detecção. A lista de plataformas disponíveis é determinada pelas vulnerabilidades atualizadas através da ferramenta Patch e conformidade. Clique em **Carregar lista padrão de plataforma** para acrescentar as plataformas disponíveis à lista. É necessário selecionar pelo menos uma plataforma.

7. Na página Produtos afetados, associe a regra com um ou mais aplicativos específicos de software. Primeiro, clique em **Editar** para abrir a caixa de diálogo Produtos afetados selecionados onde poderá acrescentar e remover produtos na lista Produtos afetados (esta lista pode ser diminuída, selecionando na caixa de seleção na parte inferior da caixa de diálogo). A lista de produtos disponíveis é determinada pelo conteúdo que você atualizou. Não é necessária a associação de um produto com uma regra de detecção. Os produtos associados agem como um filtro durante o processo de análise de segurança. Se o produto associado específico for encontrado no dispositivo, a análise é interrompida. Se o produto for encontrado, porém, ou se não houver produtos especificados, a análise continua com a verificação de arquivos.
8. Na página Arquivos, configure as condições específicas do arquivo as quais quiser que a regra analise. Clique em **Adicionar** para tornar editáveis os campos desta página. O primeiro passo na configuração de uma condição de arquivo é a especificação no método de verificação. Os campos nesta página dependem do método de verificação selecionado. Para salvar uma condição de arquivo, clique em **Atualizar**. Você pode adicionar quantas condições de arquivo desejar. Para uma descrição detalhada desta opção, consulte "Sobre a Lógica de detecção: Arquivos usados para a página de detecção" na página 630.
9. Na página Configurações do registro, configure as condições específicas do registro as quais quiser que a regra analise. Clique em **Adicionar** para tornar os campos editáveis. Para salvar uma condição do Registro, clique em **Atualizar**. Você pode adicionar quantas condições de registro desejar. Para uma descrição detalhada desta opção, consulte "Sobre a Lógica de detecção: Configurações do registro usadas para a página de detecção" na página 631.
10. Na página Script personalizado, você pode criar um script Visual Basic personalizado para ajudar esta regra de detecção. As propriedades do tempo de execução da varredura de segurança que podem ser acessadas com um script personalizado para reportar seus resultados são os seguintes: Detectado, Razão, Esperado e Encontrado.

    NOTA: Clique no botão **Usar editor** para abrir a sua ferramenta padrão de edição de script, associada a este tipo de arquivo. Quando fechar a ferramenta você será solicitado a salvar as mudanças na página Script personalizado. Se desejar usar uma ferramenta diferente é necessário mudar a associação do tipo de arquivo.

11. Na página de Informações do patch, especifique se a vulnerabilidade associada a esta regra de detecção pode ser reparada ou pode ser somente detectada nos seus dispositivos gerenciados. Se selecionou a opção de reparo, os campos Informações de download do patch e Informações de reparo se tornam editáveis.
12. Se puder reparar ao distribuir um patch, insira o URL desse arquivo patch e especifique se ele pode ser carregado automaticamente. (Você pode descarregar o arquivo de patch associado clicando em **Download** ou, se preferir, pode fazer isso outra hora.)
13. Também, se puder reparar ao distribuir um patch, insira um nome de arquivo único para o arquivo patch e especifique se o patch requer uma reinicialização para completar o reparo e se o patch requer a entrada de usuário durante o reparo. (Para uma regra de detecção que inclui consertos, recomendamos a criação de um hash para o arquivo patch ao clicar em **Gerar hash MD5**. O arquivo de patch real deve ser carregado antes da criação de um hash. Para obter mais informações sobre o hash, consulte "Sobre a Regra de detecção: Página geral de informações" na página 629.)

14. Para uma regra que permite o patch (conserto) de uma vulnerabilidade associada, você pode configurar comandos adicionais que são executados durante o processo de correção nos dispositivos afetados. Para configurar comandos adicionais de correção, clique na página Comandos de instalação do patch, em seguida clique em **Adicionar** para selecionar um tipo de comando e tornar editáveis os campos de argumento do comando. Os comandos adicionais de instalação do patch *não* são necessários. Se não configurar comandos especiais, o arquivo de conserto executa normalmente, sozinho. Para uma descrição detalhada desta opção, consulte "Sobre a página Comandos de instalação do patch" na página 634

Tendo criado uma definição de vulnerabilidade personalizada, poderá fazer o mesmo com uma vulnerabilidade de terceiros. Você pode configurar o status da vulnerabilidade como Analisar ou colocá-la no grupo Analisar a ser incluído na próxima análise de segurança, colocá-la no grupo Não analisar ou Não atribuída, ver os computadores afetados, habilitar o Reparo automático, criar um serviço de reparo ou limpar o status de análise/reparo. Para escolher uma opção, clique o botão direito numa definição de vulnerabilidade personalizada para acessar o menu de atalho.

As operações exclusivas às definições configuradas pelo usuário são importação, exportação e exportação.

Exclusão de definições personalizadas

Se não precisar mais da definição personalizada, elimine-a. Excluir uma definição personalizada remove as suas informações e regras de detecção associadas do banco de dados núcleo e da janela Patch e conformidade. (A exportação não remove as informações de definição.)

Assim como na purgação de informações de vulnerabilidade conhecida, a exclusão das definições personalizadas não remove os arquivos de patch associados. Os arquivos de patch devem ser removidos do repositório de patch manualmente.

Para excluir definições personalizadas, selecione uma ou mais definições, em seguida clique no botão da barra de ferramentas **Excluir definições personalizadas selecionadas**.

NOTA: Restauração das definições personalizadas exportadas
Se excluiu uma definição personalizada que foi exportada anteriormente como arquivo XML, você pode restaurá-la ao importá-la de volta para o banco de dados através da ferramenta Patch e conformidade.

Importar e exportar definições personalizadas

A ferramenta Patch e conformidade possibilita a importação e exportação de definições personalizadas e suas regras de detecção. Não é possível importar e exportar definições de vulnerabilidade conhecidas da indústria.

As definições personalizadas são exportadas e importadas como arquivos no formato XML.

A importação e exportação são úteis se quiser compartilhar definições personalizadas com outros servidores núcleo. A exportação possibilita salvar uma cópia backup para uma definição que quiser remover temporariamente do banco de dados núcleo.

O recurso de exportação/importação também pode ser usado para exportar uma definição, editar manualmente o arquivo exportado como modelo e salvar variações da definição, para depois importar as novas definições. Se a definição for complexa, este procedimento pode ser mais rápido e mais fácil do que a criação de várias definições no console.

Para exportar definições personalizadas

1. Na lista Definições personalizadas, selecione uma ou mais definições.
2. Clique no botão da barra de ferramentas **Exportar**. (Ou clique com o botão direito nas definições selecionadas e, em seguida, clique em **Exportar**.)
3. Insira o caminho à pasta onde quiser exportar as definições como um arquivo XML.
4. Se tiver exportado as definições anteriormente ao local especificado e quiser substituí-la, clique em **Sobrescrever definições existentes**.
5. Clique em **Exportar** e verifique a janela Status da exportação para confirmar se as definições foram exportadas com êxito.
   NOTA: Uma definição exportada continua a existir no banco de dados núcleo, assim sendo, ela ainda aparece no grupo Definições personalizadas que corresponde ao seu status: Não atribuída, Analisar ou Não analisar.
6. Clique em **Fechar**.

Para importar definições personalizadas

1. No Patch e conformidade, clique no botão da barra de ferramentas **Importar definições personalizadas**.
2. Localize e selecione uma ou mais definições (no arquivo XML que quiser importar), em seguida clique em **Abrir**. Se a definição já existir no banco de dados do núcleo, um mensagem solicitando que você confirme se deseja sobrescrevê-la. Verifique a janela de status para confirmar se a definição foi importada com êxito.
3. Clique em **Fechar**. As Definições importadas (novas e atualizadas) são colocadas no grupo Definições personalizadas não atribuídas.

Visão geral de análises de segurança

Tradicionalmente, a análise de segurança significava verificar as versões instaladas de arquivos específicos do sistema operacional e dos aplicativos, bem como verificar as chaves de registro em um dispositivo referente às vulnerabilidades conhecidas mais recentes para identificar e resolver os riscos de segurança. O LANDesk Security Suite oferece tipos de conteúdo expandido de segurança e patch, possibilitando análise e correção dos riscos de segurança predominantes atuais assim como exposições de segurança.

Dependendo da sua assinatura de conteúdo do Security Suite, você pode analisar:

- Vulnerabilidades conhecidas (para Windows, Mac, Linux e UNIX)
- Vulnerabilidades personalizadas (definidas por um Administrador LANDesk)
- Spyware
- Status de análise antivírus (mecanismos de análise de terceiros, assim como a ferramenta do LANDesk Antivirus)
- Vírus (usando a ferramenta integrada LANDesk Antivirus é possível: fazer o download os arquivos de definições de vírus mais recentes, criar e distribuir análises antivírus, configurar definições de análise de antivírus e as opções de análise de antivírus disponíveis aos usuários finais, habilitar proteção de arquivo e e-mail em tempo real, entre outros. Para obter mais informações, consulte "LANDesk Antivirus" na página 712.)
- Ameaças de segurança (erros de configuração de sistema local ou de plataforma; inclui detecção e configuração de firewall)
- Aplicativos bloqueados

- Atualizações de software LANDesk
- Atualizações de drivers
- Atualizações de software

IMPORTANTE: Assinaturas do conteúdo do LANDesk Security Suite
Para obter informações sobre assinaturas de conteúdo do Security Suite, entre em contato com um representante ou visite o site da LANDesk:
LANDesk Home Page

Tópicos relacionados

"Como as análises de Patch e conformidade para diferentes riscos de segurança" na página 589

"Criar tarefas de análise de segurança e conformidade" na página 591

"Configurar opções de análise com parâmetros de análise e reparo" na página 593

"Configurar o conteúdo de análise de segurança" na página 591

"Exibir dados de segurança detectados" na página 596

"Visão geral da correção de segurança" na página 598

Como as análises de Patch e conformidade para diferentes riscos de segurança

A tabela abaixo descreve como Analisador de segurança de patch e conformidade busca por cada tipo de risco de segurança:

Quando estiver analisando...	Análises de patch e conformidade por...
Atualizações de software LANDesk	Uso de definições de atualização de software publicadas pela LANDesk para checar as versões mais recentes de software LANDesk.
Vulnerabilidades do Windows	Usa definições de vulnerabilidade publicadas pela LANDesk (baseadas em boletins oficiais de segurança do fornecedor) para detectar vulnerabilidades conhecidas do sistema operacional e/ou do aplicativo.
Vulnerabilidades do Macintosh	Usa definições de vulnerabilidade publicadas pela LANDesk (baseadas em boletins oficiais de segurança) para verificar as vulnerabilidades conhecidas.
Vulnerabilidades do Linux/UNIX	Usa definições de vulnerabilidade publicadas pela LANDesk (baseadas em boletins oficiais de segurança) para verificar as vulnerabilidades conhecidas.
Definições personalizadas	Usa definições de vulnerabilidade personalizadas, criadas por Administradores LANDesk para verificar uma plataforma definida pelo usuário, aplicativo, arquivo ou condições de configuração do registro.

Quando estiver analisando...	Análises de patch e conformidade por...
Riscos de segurança	Uso de definições riscos de segurança publicadas pela LANDesk para verificar erros e exposições de configuração do sistema local Windows. Você pode modificar as definições de riscos de segurança que usam variáveis personalizadas editáveis para checar condições específicas.
Spyware	Usa definições de detecção spyware que verifica as instâncias de programas de spyware nos dispositivos analisados. O Patch e conformidade utiliza a ferramenta de monitoração de licença do LANDesk Software, softmon.exe, para monitorar spyware. É possível também habilitar a monitoração e o bloqueamento de spyware em tempo real com uma configuração do agente do dispositivo.
Atualizações de drivers	Usa definição de atualização de driver de terceiros que procuram versões de drivers.
Atualizações de software	Usa definições de atualização de software de terceiros que procuram versões de software.
Atualizações de antivírus	Usa definições de detecção do analisador de antivírus (NÃO os arquivos reais de definição/padrão de vírus) que verificam: - instalação de mecanismos comuns de análise de antivírus (inclusive a ferramenta LANDesk Antivirus) - status de análises em tempo real (habilitada ou desabilitada) - versões de arquivo de padrões específicos à análise (atualizada ou antiga) - última data de análise (se a última análise está dentro do período máximo permitido especificado pelo administrador)
Aplicativos bloqueados	Usa definições de aplicativo publicadas pela LANDesk (ou definições de aplicativos criadas pelo usuário) para imediatamente negar ao usuário final o acesso ao aplicativo através da edição do registro local. A correção não é um procedimento separado. O Patch e conformidade utiliza o recurso da ferramenta de monitoração de licença do LANDesk Software, o programa softmon.exe, para negar o acesso a executáveis de aplicativos especificados mesmo se o nome de arquivo do executável tiver sido modificado, ao ler as informações do cabeçalho do arquivo.

Para compreender como o Patch e conformidade corrige esses diferentes tipos de conteúdo, consulte "Métodos de correção" na página 603.

Configurar o conteúdo de análise de segurança

Após rever as definições de download e decidir quais itens quer analisar, você pode fazer uma avaliação de segurança personalizada nos dispositivos gerenciados ao mover as definições nos respectivos grupos de análise. Sempre que o analisador de segurança é executado, ele lê o conteúdo do grupo de Análise e busca por aquelas definições específicas (mas *só* se esse tipo for selecionado na análise da tarefa e nas configurações de reparo). Antes de analisar os dispositivos, certifique-se sempre de que as definições apropriadas estão no grupo Analisar. Você pode mover as definições manualmente, a qualquer momento, dentro e fora do grupo Analisar.

Também pode atualizar o conteúdo de segurança que, por padrão, acrescenta automaticamente novas definições no grupo Analisar.

IMPORTANTE: Os aplicativos bloqueados são colocados no grupo Não atribuídas por padrão
Lembre-se de que o tipo de aplicativo bloqueado é tratado de modo diferente dos outros tipos. Como padrão, as definições bloqueadas de aplicativo são colocadas no grupo Não atribuídas, e não no grupo Analisar.

As análises de segurança adicionam informações de patch e conformidade ao inventário de um dispositivo no banco de dados núcleo. Essas informações podem ser usadas para gerar consultas, diretivas e relatórios específicos. Para ver essas informações, clique com o botão direito no dispositivo e, em seguida, clique em **Informações de segurança e patch**.

CUIDADO: Mover definições do grupo Analisar
Ao mover definições do grupo Analisar para o grupo Não analisar, as informações atuais de avaliação de definição (localizadas no banco de dados núcleo sobre quais os dispositivos analisados detectaram essas definições) são removidas do banco de dados núcleo e não ficam mais disponíveis na caixa de diálogo Propriedades ou Informações de Segurança e Patch do dispositivo. Para restaurar essas informações, você deve mover as definições de volta ao grupo Analisar e executar novamente a análise.

Criar tarefas de análise de segurança e conformidade

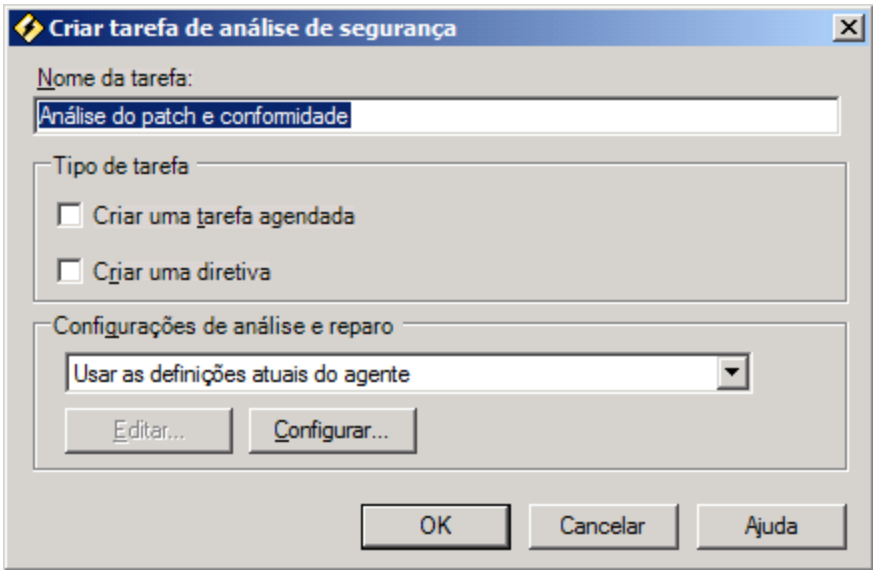
O analisador de segurança pode ser executado diretamente em um dispositivo (Clique em **Iniciar > Todos os programas > LANDesk Management > Analisador de segurança**). O analisador de segurança pode também ser executado como uma tarefa agendada ou diretiva do servidor núcleo.

IMPORTANTE: Permissões de grupos LANDesk Script Writers são necessárias
Para criar tarefas agendadas e diretivas na ferramenta Patch e conformidade e a ferramenta Configurações de segurança (para tarefas de análise de segurança e conformidade, tarefas de reparo e tarefas de mudanças de configurações), um usuário precisa ter permissão de grupo LANDesk Script Writers. Em outras palavras, eles precisam pertencer a um grupo que tenha permissão de LANDesk Script Writers atribuída. Para obter mais informações sobre a administração baseada em funções, consulte "Gerenciamento de usuários" na página 38.

As tarefas agendadas podem ser consideradas uma distribuição de instalação, pois a tarefa é instalada do servidor núcleo para os dispositivos, enquanto que uma diretiva é considerada uma distribuição forçada, pois o agente de diretivas nos dispositivos verifica o servidor núcleo quanto às diretivas aplicáveis e então "instala" o patch a partir do servidor núcleo.

Para criar uma tarefa de análise de segurança

1. Clique em **Ferramentas > Patch e conformidade**.
2. Certifique-se de que as informações de conteúdo de segurança tenham sido atualizadas recentemente.
3. Certifique-se que o grupo **Analisar** contém somente as definições que quiser analisar.
4. Clique no botão **Criar uma tarefa** da barra de ferramentas e clique em **Análise de segurança**. A caixa de diálogo Criar tarefa de análise de segurança é mostrado.



5. Digite um nome para a análise.
6. Especifique se a análise é uma tarefa agendada ou uma análise baseada em diretivas, ou ambas.
7. Selecione uma das configurações de análise e reparo na lista disponível (ou crie configurações personalizadas para esta análise) para determinar como a análise funciona nos dispositivos do usuário final.
8. Clique em **OK**. Para uma análise agendada da tarefa, agora você pode acrescentar dispositivos de origem e configurar as opções de agendamento na ferramenta Tarefas agendadas.

NOTA: Análises de segurança de conformidade
Com a ferramenta Patch e conformidade você pode criar uma tarefa de análise de conformidade específica, que verifica os dispositivos alvo para conformidade com a sua diretiva de segurança personalizada. Uma análise de conformidade é baseada no conteúdo do grupo **Conformidade** (e as opções especificadas nas configurações de conformidade) e pode ser executada como tarefa agendada, diretiva e até iniciada pelo LANDesk Antivirus quando um vírus é detectado, o qual não pode ser removido ou ser colocado em quarentena.

Análises de segurança e conformidade por demanda

Você pode também executar uma análise imediata por demanda em um ou mais dispositivos alvo.

Para fazer isso, clique com o botão direito no dispositivo selecionado (ou até 20 dispositivos selecionados em conjunto), clique em **Análise de Security/Conformidade LanDesk agora**, selecione definições de análise e reparo, o tipo de análise e clique em **OK**.

Sobre o arquivo de log de análise de segurança

A análise de security grava um arquivo de log para a análise mais recente do dispositivo chamado **vulscan.log** e também salva os últimos cinco arquivos de log em ordem cronológica por número. Esses arquivos de log registram informações úteis sobre a hora da análise, o idioma, a plataforma e os processos executados pela análise.

Visualizar as datas de análise de segurança mais recentes no inventário do dispositivo

Para ver quando a última análise de segurança foi executada em um dispositivo, clique com o botão direito no dispositivo, clique em **Inventário** e, em seguida, role para baixo até **Últimas datas de análise** no painel direito da tela Inventário.

Configurar opções de análise com parâmetros de análise e reparo

O Patch e conformidade lhe dá controle completo sobre o que o usuário final vê, sobre o comportamento de reinicialização do dispositivo e o nível de interação permitido ao usuário quando a análise de segurança é executada nos dispositivos. Por exemplo, dependendo do propósito ou da hora agendada de uma análise, pode ser útil mostrar o andamento da análise ao usuário final e lhe dar a oportunidade de cancelar ou pospor uma análise de avaliação ou correção de distribuição do patch. Você pode fazer isso criando e aplicando configurações de análise e reparo.

As configurações de análise e reparo é também onde você determina o conteúdo de uma análise de segurança selecionando tipos específicos de definições.

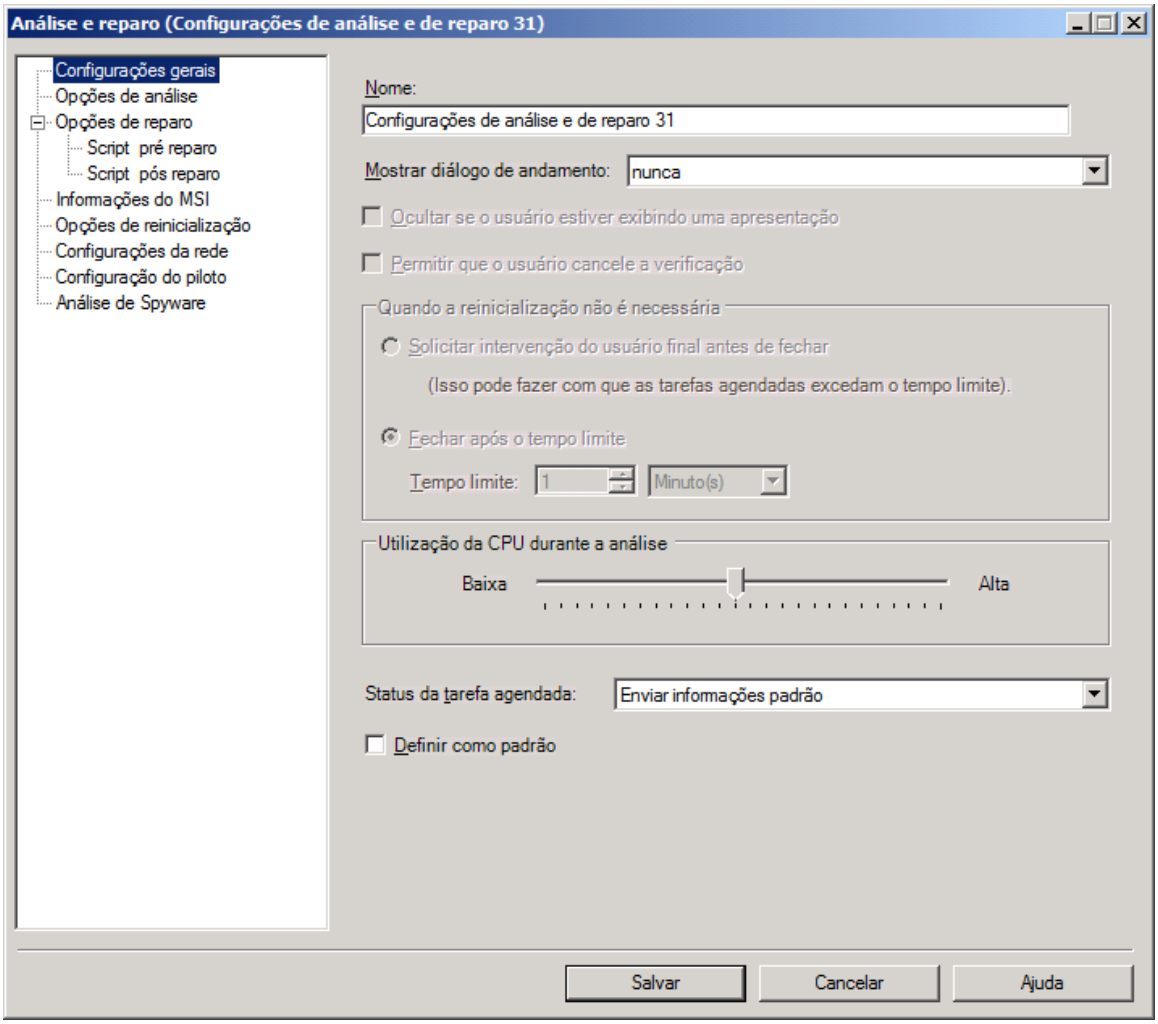
Crie e aplique as configurações de análise e reparo (um conjunto salvo de opções configuradas) às tarefas de análise. Você pode criar quantas configurações de análise e reparo quiser. Algumas configurações de análise e reparo podem ser perfeitas para uma variedade de tarefas de análise ou correção, enquanto outras podem ter sido criadas especificamente para uma única tarefa.

Todas as configurações de análise e reparo são armazenadas no grupo **Análise e reparo** localizados em **Configurações** na tela da árvore.

Para criar configurações de análise e reparo

1. Na janela da ferramenta do **Patch e conformidade**, clique no botão **Configurar definições** da barra de ferramentas e, em seguida, clique em **Configurações de análise e reparo**.

2. Clique em **Nova**. Ou clique em **Editar** ou **Configurar** em qualquer caixa de diálogo de tarefas que permite aplicar uma configuração de análise e reparo.



3. Digite um nome para as configurações de análise e reparo.
4. Especifique as várias configurações em cada página como desejado para a tarefa em particular (analisar, reparar, inicializar). Clique em **Ajuda** para obter mais informações sobre uma opção.

Quando definidas, você pode aplicar as configurações de análise e reparo às tarefas de análise de segurança, tarefas de reparo, tarefas de desinstalação e tarefas de reinicialização e tarefas de mudança de definições.

NOTA: Configurações de conformidade
Com a ferramenta Patch e conformidade você pode também criar configurações específicas de conformidade que determinam quando a análise frequente de segurança é executada e como os riscos detectados são corrigidos. Uma análise de conformidade é baseada no conteúdo do grupo **Conformidade** (e as opções especificadas nas configurações de conformidade) e pode ser executada como tarefa agendada, diretiva e até iniciada pelo LANDesk Antivirus quando um vírus é detectado, o qual não pode ser removido ou ser colocado em quarentena.

Mudar configurações padrão de análise e reparo de um dispositivo

As configurações padrão de análise e reparo de um dispositivo são distribuídas como parte da configuração inicial do agente. Quando uma tarefa tem configurações de análise e reparo diferentes associadas ou atribuídas a ela, as configurações padrão são canceladas. Se preferir, você pode usar as configurações padrão selecionando-as ao criar uma tarefa.

Para determinados dispositivos, porém, você pode decidir mudar essas configurações de análise e reparo padrão. O Patch e Conformidade fornece um meio de fazer isso sem ter que redistribuir uma configuração nova e completa. Para fazer isso, use a tarefa **Mudar configurações** localizada no botão **Criar uma tarefa** da barra de tarefas.

A caixa de diálogo que aparece e permite digitar um nome exclusivo para a tarefa, especificar se se trata de uma tarefa agendada ou de uma diretiva e selecionar uma configuração de análise e reparo existente como padrão ou usar o botão **Editar** para criar uma nova configuração de análise e reparo como padrão para os dispositivos alvo.

Usar variáveis personalizadas e configurações de substituição de variáveis personalizadas

Com as variáveis personalizadas é possível ajustar a análise de ameaça de segurança modificando um ou mais valores para que o analisador verifique as condições definidas e determine um dispositivo para ser vulnerável somente se aquela condição for satisfeita (por exemplo, o valor especificado é detectado). Algumas definições de ameaça de segurança de configuração de sistema têm parâmetros que foram mudados antes de incluí-las na análise de segurança. Normalmente, as definições de antivírus têm também configurações variáveis personalizadas.

IMPORTANTE: É necessário editar o direito Variáveis personalizadas
Para editar as configurações de variáveis personalizadas, o usuário LANDesk deve ter o direito de administração com base em função Editar variáveis personalizadas. Os direitos são configurados com a ferramenta **Usuários**.

Cada definição de segurança com variáveis personalizadas tem um conjunto exclusivo de valores específicos que podem ser modificados. Entretanto, em cada caso, a página **Variáveis personalizadas** mostrará as seguintes informações comuns:

- **Nome:** Identifica a variável personalizada. O nome não pode ser modificado.
- **Valor:** Indica o valor atual da variável personalizada. A menos que a variável seja de apenas leitura, você pode clicar duas vezes nesse campo para mudar o valor.
- **Descrição:** Fornece mais informações úteis sobre a variável personalizada do editor de definição.
- **Valor padrão:** Fornece o valor padrão caso você tenha mudado as configurações e deseja restaurá-las ao valor original.

Para alterar uma variável personalizada, clique duas vezes no campo **Valor** e selecione um valor se houver uma lista disponível ou edite manualmente o valor, e clique em **Aplicar**. Observe que algumas variáveis são apenas leitura e não podem ser editadas (normalmente indicado na descrição).

NOTA: Configurações de variáveis personalizadas a serem substituídas
Em algumas situações, talvez você queira ignorar as configurações de variável personalizada ou, em

outras palavras, criar uma exceção à regra. É possível fazer isso com o recurso de configurações de substituição de variáveis personalizadas. As configurações para substituir as variáveis personalizadas permitem decidir quais variáveis deverão ser ignoradas ao analisar dispositivos para que eles não sejam detectados como vulneráveis e corrigidos mesmo que atendam às condições de regras de detecção de uma definição. O usuário precisa ter o direito Editar variáveis personalizadas para poder criar ou editar configurações de substituição de variáveis personalizadas. Você pode criar quantas definições desejar e aplicá-las aos dispositivos usando uma tarefa **Mudar configurações**. Para obter mais informações, consulte "Sobre a caixa de diálogo Configurar as definições da variável personalizada a ser substituída" na página 650.

Exibir dados de segurança detectados

Se o analisador de segurança descobrir uma das definições selecionadas de vírus nos dispositivos alvo, essa informação é reportada ao servidor núcleo. Você pode usar qualquer um dos métodos abaixo para exibir dados de segurança detectados após executar uma análise:

Pelo grupo Detectadas

Na janela da ferramenta Patch e conformidade, selecione o grupo **Detectadas** para ver uma lista completa de todas as vulnerabilidades detectadas pela análise mais recente.

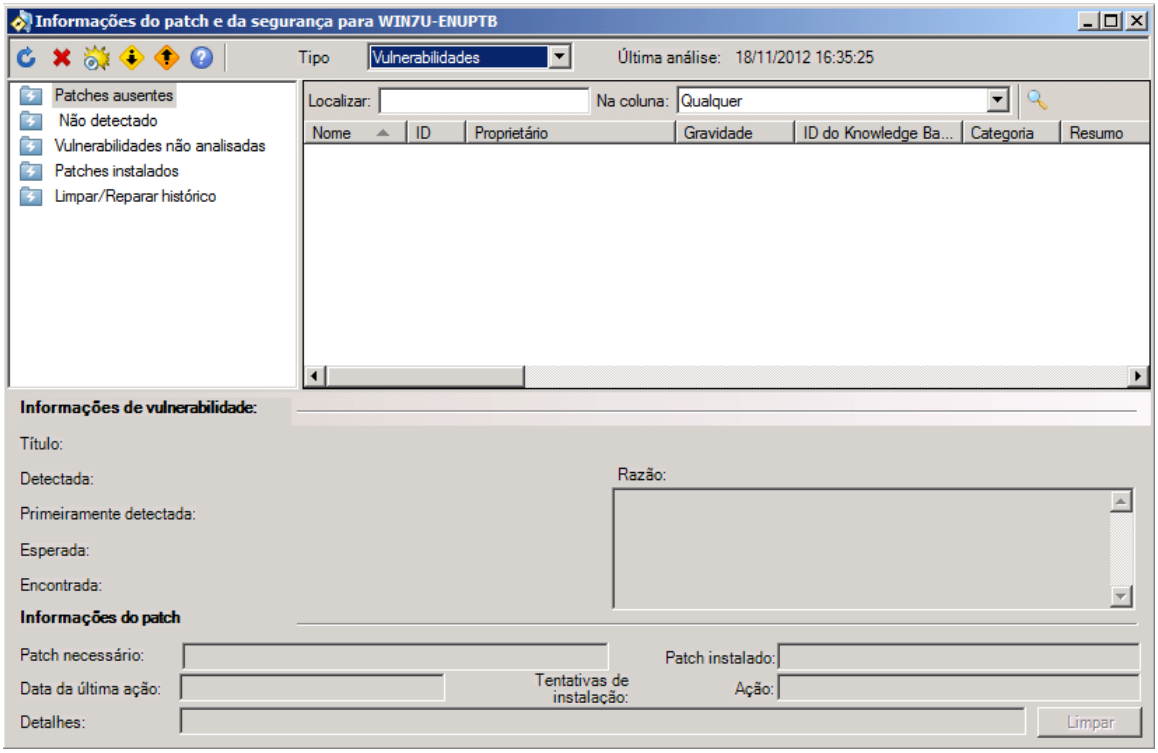
A coluna Analisados indica quantos dispositivos foram analisados para uma definição e a coluna Detectados mostra quantos desses dispositivos são afetados por essa definição.

Por uma definição

Clique com o botão direito em uma definição e, em seguida, clique em **Computadores afetados** para ver uma lista dos dispositivos nos quais a definição foi detectada pela análise mais recente.

De acordo com a caixa de diálogo Informações de segurança e patch do dispositivo

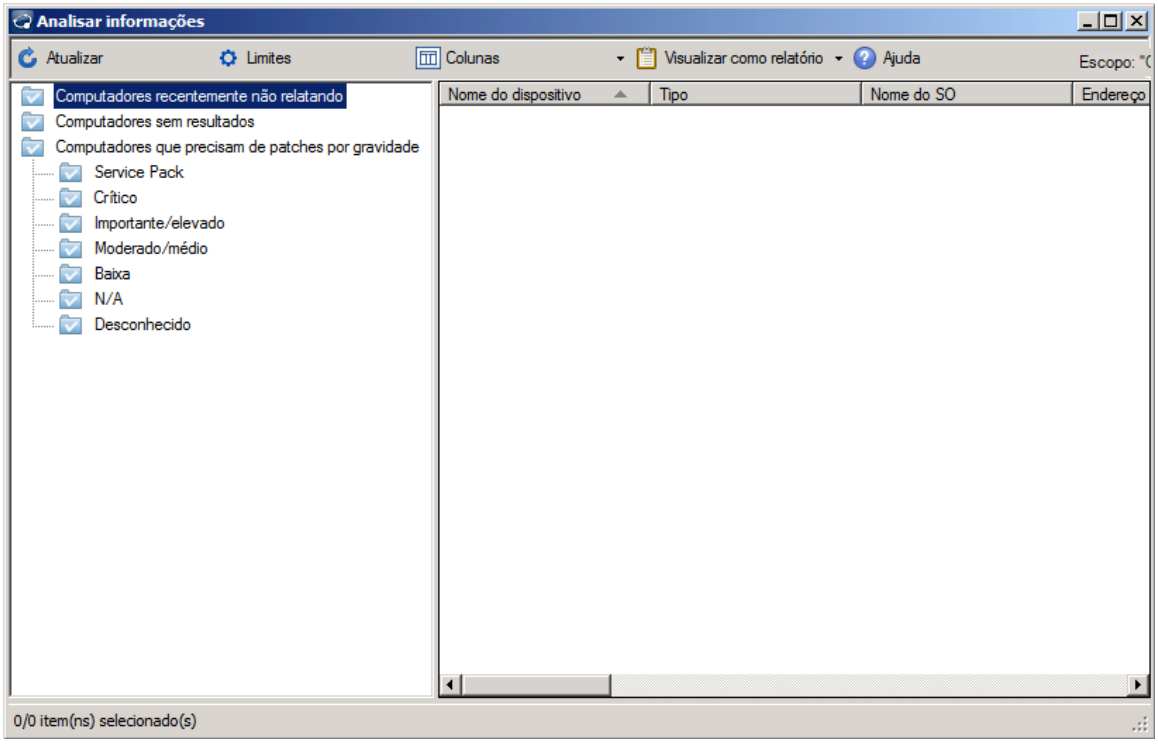
Clique com o botão direito em um dispositivo específico na tela da rede, em seguida clique em **Informações de segurança e patch** para ver as informações detalhadas sobre a avaliação de segurança e o status de distribuição do patch para o dispositivo.



Você pode também selecionar múltiplos dispositivos na tela de rede, clique com o botão direito no grupo e, em seguida, clique em **Informações de segurança e patch** para exibir uma lista das definições descobertas em um ou mais desses dispositivos. Quando você seleciona uma definição na lista, os dispositivos nos quais a definição foi detectada pela análise mais recente são mostrados no painel inferior.

De acordo com a caixa de diálogo Informações da análise

Na janela da ferramenta Patch e conformidade, clique no botão da barra de ferramenta **Informações da análise** para ver a atividade detalhada de distribuição de patch e o status dos dispositivos analisados na sua rede. Você pode ver os resultados da análise para computadores que não forneceram informações recentemente, computadores sem resultados e computadores que precisam de patches por tipo de gravidade selecionada.



Encaminhar resultados da análise de segurança a um núcleo rollup

Se você estiver trabalhando em uma grande rede empresarial distribuída, talvez queira enviar os resultados mais recentes da análise de segurança a um servidor núcleo de rollup localizado numa região específica. Isso facilitará o acesso às informações de vulnerabilidade em tempo real para todos os dispositivos gerenciados. Você pode habilitar resultados de análise (vulnerabilidade) de segurança imediata e automática ao definir configurações na ferramenta Patch e conformidade.

Sempre que a análise de segurança é executada, ela grava um arquivo de resultados da análise em uma pasta chamada VulscanResults no servidor núcleo e notifica o serviço Web do LANDesk Security Suite que adiciona o arquivo ao banco de dados núcleo. Se as configurações do núcleo de rollup forem habilitadas e um núcleo válido de rollup é identificado, o núcleo de rollup lê o arquivo de resultados da análise em seu banco de dados, fornecendo acesso mais rápido às informações de vulnerabilidade crítica.

Para habilitar o envio imediato dos resultados da análise de segurança para um núcleo de rollup

1. Na janela da ferramenta do **Patch e conformidade**, clique no botão **Configurar parâmetros** da barra de ferramentas e, em seguida, clique em **Configurações de núcleo de rollup**.
2. Marque a caixa de seleção **Enviar resultados da análise ao núcleo de rollup imediatamente**.
3. Insira o nome do núcleo de rollup do qual você quer receber os resultados mais recentes de análise de segurança.
4. Se quiser usar o URL padrão (local do núcleo de rollup) onde o arquivo de resultados da análise está gravado, marque a caixa de seleção **Utilizar URL padrão do rollup**. Caso contrário, desmarque a caixa de seleção e insira o endereço preferencial.

Visão geral da correção de segurança

Esta seção oferece uma visão geral sobre dispositivos de correção que detectaram riscos de segurança.

Quando tiver atualizado o conteúdo de segurança para os tipos de conteúdo licenciados ou para os quais tiver assinatura e os dispositivos analisados, determinado quais exposições de segurança detectadas requerem atenção e descarregado os patches, a próxima etapa na implementação do Patch e conformidade é a correção (ou reparo) do problema de segurança).

As soluções e ações de correção são diferentes, dependendo do tipo do risco e segurança. Além disso, algumas correções podem ser feitas remotamente com a ferramenta Patch e conformidade, enquanto que outras tarefas de detecção precisam ser feitas manualmente. Por exemplo, as vulnerabilidades são corrigidas com a distribuição e instalação dos patches de segurança necessários nos dispositivos afetados, enquanto que o spyware é corrigido com a remoção do próprio spyware e a ameaça de segurança de configuração do sistema é normalmente corrigida com edição do registro ou pela mudança de algumas configurações específicas da plataforma.

Correção para diferentes riscos de segurança

A correção para cada tipo de risco de segurança (ou tipo de conteúdo) é descrito abaixo:

Vulnerabilidades conhecidas

Para vulnerabilidades conhecidas, a correção é a distribuição e instalação do patch apropriado de segurança. A correção de vulnerabilidade do Windows e Macintosh pode ser feita através do console, como uma tarefa agendada ou correção baseada em diretiva, ou ainda como análise de reparo automático. Entretanto, a correção da vulnerabilidade Linux e UNIX deve ser feita manualmente no dispositivo afetado.

Definições personalizadas

Para as definições personalizadas, a correção pode consistir na distribuição de um patch personalizado ou script que trata da exposição. Como a correção conhecida de vulnerabilidade, as tarefas de reparo de vulnerabilidade personalizadas podem ser feitas através do console.

Atualizações de software LANDesk

Para as atualizações de software da LANDesk, a correção significa que a versão de atualização apropriada está instalada. Isso pode ser feito através do console.

Riscos de segurança

Para riscos de segurança (erros e exposições de configuração de sistema Windows local ou plataforma), correção signfica aplicar os parâmetros de configuração especificados pela definição de risco de segurança. Isso pode ser feito através do console. Você pode modificar as definições de riscos de segurança que usam variáveis personalizadas para aplicar as derfinições personalizadas.

Alguns riscos de segurança precisam ser corrigidos manualmente no dispositivo afetado. Para saver se um risco de segurança pode ser corrigido do console, veja o seu valor de coluna Reparável (Sim ou Não) na tela de lista de item.

A detecção e configuração de firewall (usando configurações de firewall Windows e definições de risco de segurança)

Para as configurações de firewall do Windows, correção significa aplicar definições de configuração especificadas por configurações de firewall do Windows ou definições de risco de segurança pré-definidas.

As configurações de firewall de Windows são associadas a uma tarefa para habilitar/desabilitar a firewall e configurar os parâmetros de configuração incluindo exceções, regras de entrada e regras de saída (para serviços, portas, programas) nos dispositivos alvo que executam as seguintes plataformas Windows:

- Windows 2003/XP
- Windows Vista

Além disso, o LANDesk Security Suite fornece definições de risco de segurança pré-definidas que lhe permitem analisar, detectar e configurar parâmetros de firewall em dispositivos gerenciados que executam plataformas Windows executivas. As seguintes definições de ameaça de segurança permitem que você faça uma análise em busca de e modifique as configurações de firewall:

- **ST000102:** Definição de ameaça de segurança para a firewall Windows em Windows 2003 SP1; Windows XP SP2.
- **ST000015:** Definição de ameaça de segurança para Firewall de conexão de Internet no Windows 2003 SP1; Windows XP SP2.

As propriedades de ameaça de segurança da firewall do Windows incluem variáveis personalizadas que permitem configurar parâmetros do firewall do Windows. Você pode usar essas definições de ameaça de segurança para analisar e procurar parâmetros especificados e retornar uma condição de vulnerabilidade se esses parâmetros não forem correspondidos. Use, então, a definição personalizada em uma tarefa de reparo para ativar ou desativar a firewall e mudar ou reconfigurar os parâmetros da firewall no dispositivo analisados.

CUIDADO: O Windows GPO pode mudar configurações de firewall
É possível que o Windows Group Policy Object (GPO) interfira com as configurações da firewall configuradas com o analisador de segurança. Por exemplo, as configurações de firewall que você define na caixa de diálogo Configurar variáveis personalizadas da ameaça de segurança do Windows Firewall que são implantadas por uma tarefa de reparo da análise de segurança, podem ser restauradas aos seus valores originais conforme as configurações foram definidas em um Objeto de diretiva de grupo.

Spyware

Para o spyware, a correção consiste na remoção do aplicativo spyware invasor. Isso pode ser feito remotamente do console com uma tarefa de reparo.

Você pode também configurar um dispositivo para a monitoração de spyware em tempo real (análise, detecção e remoção). Para usar a monitoração de spyware em tempo real é necessário ativar as configurações na configuração de agente do dispositivo. Na página **Spyware** da caixa de diálogo **Configuração do agente**, selecione as opções apropriadas de monitoração para habilitar a monitoração de spyware em tempo real e a notificação do usuário final. A monitoração de spyware em tempo real usa o programa softmon.exe da ferramenta de monitoração de licença LANDesk Software para monitorar spywares e criar arquivos de registro lidos pelo analisador de segurança durante a análise as definições de spyware nos dispositivos alvo.

IMPORTANTE: A correção automática deve estar ativada para a monitoração de spyware em tempo real
Para a análise e detecção de spyware em tempo real funcionar, as definições descarregadas de spyware devem ter a opção de correção automática ativada. Você ativa manualmente a opção de correção automática para as definições de spyware nas listas de itens da janela da ferramenta Patch e conformidade. Ou pode também configurar as atualizações de definição de spyware para que a correção automática seja ligada como padrão quando as definições de spyware forem descarregadas.

Aplicativos bloqueados

Para aplicativos bloqueados, a correção NÃO é uma tarefa separada. O bloqueio de aplicativos ocorre como parte da própria análise de segurança, com a edição do registro no disco rígido local para desativar o acesso do usuário a qualquer aplicativo não autorizado.

O Patch e conformidade usa o programa softmon.exe, para negar o acesso aos executáveis de aplicativos especificados ao ler as informações do cabeçalho do arquivo, mesmo se o nome de arquivo do executável tiver sido modificado

Atualizações de antivírus

As atualizações de antivírus estão disponíveis para vários produtos comuns de antivírus, inclusive o LANDesk Antivirus. Consulte a lista **Tipos de definições** na caixa de diálogo **Download de atualizações** para ver os mecanismos de análise antivírus suportados, isto é, os analisadores antivírus para os quais você pode descarregar definições de detecção.

NOTA: Conteúdo de detecção do analisador de antivírus comparado com o conteúdo de definições
As atualizações de antivírus não implicam na existência de arquivos de definição (ou padrões) de vírus. Quando você faz o download das atualizações antivírus de terceiros, apenas o conteúdo de detecção do analisador é baixado para o repositório padrão, mas NÃO os arquivos de definição de vírus específicos do analisador. Entretanto, ao fazer o download das atualizações do LANDesk Antivirus, o conteúdo de detecção do analisador e as atualizações do arquivo de definições de vírus do LANDesk Antivirus são baixados. Os arquivos de definição de vírus do LANDesk Antivirus são baixados em um local separado no servidor núcleo. O repositório padrão do arquivo de definições de vírus é a pasta \LDLogon\Antivirus\Bases.

Atualizações de antivírus são definições de análise que detectam:

- instalação de mecanismos de análise antivírus comuns (incluindo a ferramenta LANDesk Antivirus)
- status de análise em tempo real (ativado ou desativado)
- versões do arquivo de padrões específicos do analisador (atualizado ou antigo)
- data da última análise (se a análise mais recente estiver dentro do período máximo permitido especificado pelo administrador)

Quando você distribui uma análise de segurança com as definições de detecção antivírus, o analisador de segurança (1) verifica se o mecanismo de análise antivírus está instalado nos dispositivos gerenciados, (2) se a análise em tempo real está ativada ou desativada, (3) se os arquivos de padrões do analisador está atualizado e (4) quando foi executada a última análise no dispositivo. A análise antivírus em tempo real pode ser executada remotamente, se estiver desativada.

Como o Patch e conformidade corrige diferentes riscos de segurança

A tabela a seguir descreve como o Patch e conformidade corrige cada tipo de risco de segurança:

Ao corrigir...	Patch e conformidade corrige por...
Atualizações de software LANDesk	Distribui e instala a atualização apropriada do software LANDesk.

Ao corrigir...	Patch e conformidade corrige por...
Vulnerabilidades do Windows	Distribui e instala os arquivos patch necessários (arquivos patch já devem ter sido descarregados no repositório de patch local).
Vulnerabilidades do Macintosh	Distribui e instala os arquivos patch necessários
Vulnerabilidades do Linux/UNIX	A correção é feita manualmente no dispositivo afetado.
Definições personalizadas	Distribui e instala os arquivos patch, se a regra de detecção associada permite a correção e se os arquivos patch especificados estiverem disponíveis.
Riscos de segurança	Aplicação de definições de configuração pela definição de ameaça de segurança. Isso pode ser feito através do console. Você pode modificar as definições de riscos de segurança que usam variáveis personalizadas para aplicar as derfinições personalizadas. Alguns riscos de segurança precisam ser corrigidos manualmente no dispositivo afetado. Para saver se um risco de segurança pode ser corrigido do console, veja o seu valor de coluna Reparável (Sim ou Não) na tela de lista de item.
Spyware	Remove a instância de spyware detectada. Consulte a seção acima sobre spyware se precisar de mais informações sobre a detecção e remoção de spyware em tempo real.
Atualizações de drivers	Distribui e instala a atualização apropriada de driver de terceiros.
Atualizações de software	Distribui e instala a atualização apropriada de software de terceiros.
Atualizações de antivírus	Permitem reativar o antivírus em tempo real se tiver sido desativado. As outras definições de detecção da análise antivírus retornam informações de status sobre instalações específicas de mecanismo de análise antivírus, versões de arquivos de padrões e as datas das últimas análises (os problemas relacionados podem ser corrigidos remotamente do console).
Aplicativos bloqueados (publicados e personalizados)	Nega o acesso ao aplicativo, mesmo se o nome de arquivo do executável do programa foi modificado, lendo as informações no cabeçalho do arquivo. A correção nesse caso não é um procedimento separado. O bloqueio de aplicativo é feito durante o processo de análise de segurança. A análise de segurança nega, imediatamente, o acesso do usuário final ao aplicativo pela edição do registro. (Consulte "Isenção de responsabilidades legais para o tipo de aplicativos bloqueados" na página 581)

Para compreender como o Patch e conformidade analisa esses diferentes tipos de conteúdo, consulte "Visão geral de análises de segurança" na página 588.

Métodos de correção

O Patch e conformidade fornece vários métodos para corrigir dispositivos afetados.

Correção inteligente da correção de distribuição de patch

O Patch e conformidade realiza uma correção inteligente instalando somente as correções necessárias em cada dispositivo. Nem todas as correções relacionadas por todas as vulnerabilidades estão incluídas na tarefa de reparo. A ferramenta também aproveita os recursos aprimorados de distribuição de pacotes da LANDesk para realizar uma distribuição rápida e eficiente dos patches, como: Multidifusão dirigida, download por parceiro e reinício do ponto de verificação. Para encontrar informações mais detalhadas sobre esses recursos de distribuição software, consulte "Distribuição de softwares/Distribuição de pacotes/Métodos de entrega" na página 258.

Correção de uma ou mais definições de cada vez

É possível corrigir uma única definição detectada ou um conjunto delas com qualquer um dos três métodos de correção descritos abaixo.

Para corrigir uma definição de cada vez, clique com o botão direito no item e, em seguida, clique em **Reparar**.

Para corrigir um conjunto de definições de uma só vez, copie-as de qualquer grupo de conteúdo para um grupo personalizado (consulte "Entenda e use a Janela da ferramenta de Patch e conformidade" na página 555), clique com o botão direito no grupo e clique em **Reparar**. O método reparo automático não está disponível para grupos personalizados; entretanto, você pode selecionar várias definições em uma lista, clicar com o botão direito e selecionar **Reparo automático**.

Correção a a partir do console

Conforme citado acima, as vulnerabilidades Windows e Macintosh, as definições personalizadas, as atualizações de software LANDesk e os aplicativos bloqueados podem ser corrigidos com o uso do console.

A correção de tarefas agendadas pode ser considerada uma distribuição de instalação, pois o patch é instalado do servidor núcleo para os dispositivos, enquanto que uma diretiva é considerada uma distribuição forçada, pois o agente de diretivas nos dispositivos verifica o servidor núcleo quanto às diretivas aplicáveis e então "instala" o patch a partir do servidor núcleo.

Use uma tarefa de reparo agendada

Agendar uma correção ou tarefa de reparo é útil se quiser configurar uma tarefa a ser executada numa hora especificada no futuro ou uma tarefa recorrente. O Patch e conformidade usa a ferramenta Tarefas agendadas para configurar e processar uma tarefa agendada de reparo.

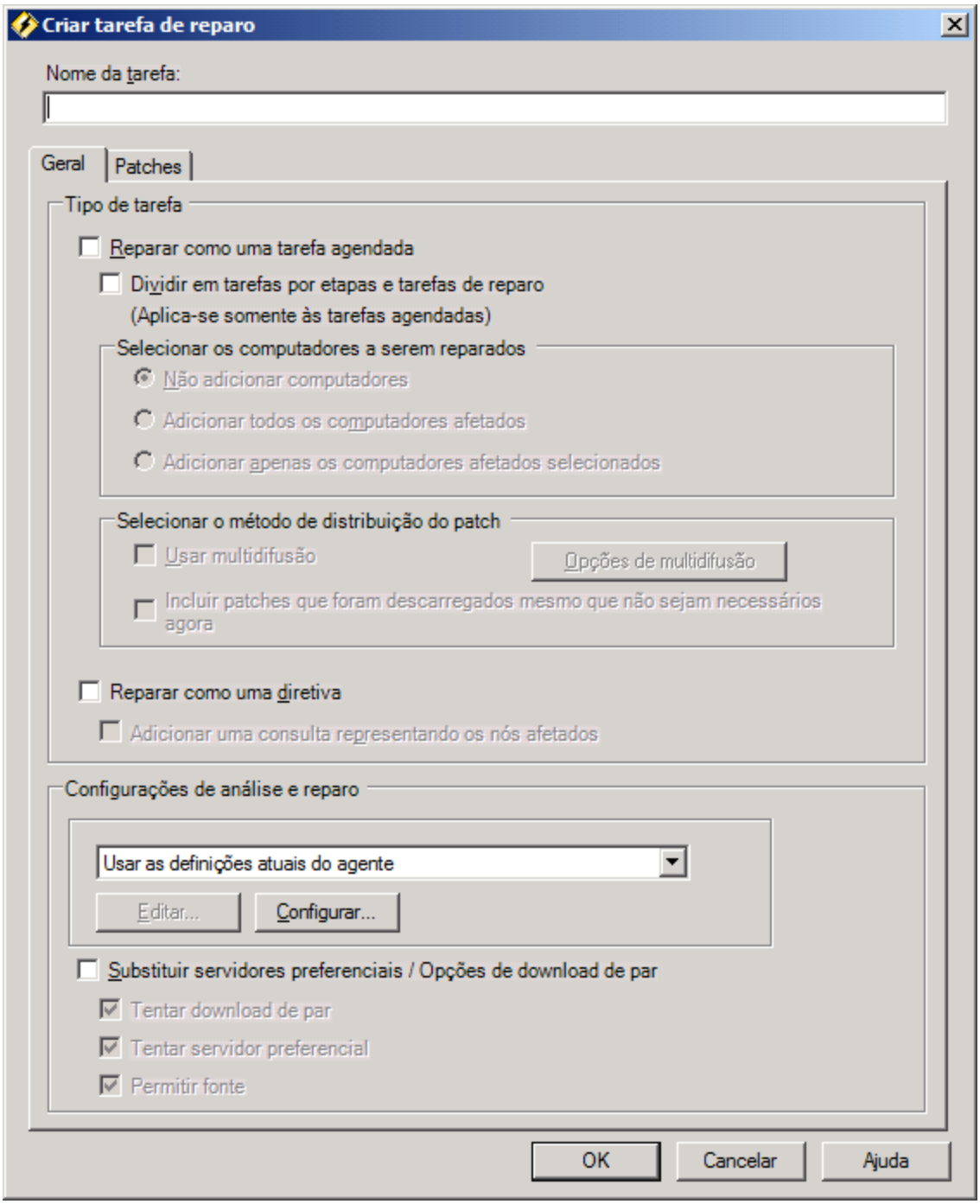
A correção de tarefa agendada é suportada nos dispositivos Windows e Macintosh.

IMPORTANTE: P**ermissões de grupos LANDesk Script Writers são necessárias**
Para criar tarefas agendadas e diretivas na ferramenta Patch e conformidade e a ferramenta Configurações de segurança (para tarefas de análise de segurança e conformidade, tarefas de reparo e tarefas de mudanças de configurações), um usuário precisa ter permissão de grupo LANDesk Script Writers. Em outras palavras, eles precisam pertencer a um grupo que tenha permissão de LANDesk Script

Writers atribuída. Para obter mais informações sobre a administração baseada em funções, consulte "Gerenciamento de usuários" na página 38.

Para criar uma tarefa agendada de reparo

1. Clique em **Ferramentas > Patch e conformidade**.
2. Clique com o botão direito em uma única definição de um dos grupos de conteúdo ou clique com o botão direito em um grupo personalizado e clique em **Reparar**. Ou, clique no botão **Criar uma tarefa** da barra de ferramentas e clique em **Reparar**. A caixa de diálogo **Criar tarefa de reparo** é exibida.


Criar tarefa de reparo
Nome da tarefa:
Geral
Patches
Tipo de tarefa
Reparar como uma tarefa agendada
Dividir em tarefas por etapas e tarefas de reparo
(Aplica-se somente às tarefas agendadas)
Selecionar os computadores a serem reparados
Não adicionar computadores
Adicionar todos os computadores afetados
Adicionar apenas os computadores afetados selecionados
Selecionar o método de distribuição do patch
Usar multidifusão
Opções de multidifusão
Incluir patches que foram descarregados mesmo que não sejam necessários agora
Reparar como uma diretiva
Adicionar uma consulta representando os nós afetados
Configurações de análise e reparo
Usar as definições atuais do agente
Editar...
Configurar...
Substituir servidores preferenciais / Opções de download de par
Tentar download de par
Tentar servidor preferencial
Permitir fonte
OK
Cancelar
Ajuda

3. Edite o **Nome da tarefa** se quiser mudar o nome da tarefa de reparo.
4. Marque a caixa de seleção **Reparar como uma tarefa agendada**.
5. (Opcional) Se quiser que essa tarefa de reparo seja dividida em duas partes (uma tarefa por etapas para distribuir os patches necessários entre os dispositivos afetados e a própria tarefa de reparo, que instala o patch), selecione **Dividir em tarefas por etapas e tarefas de reparo**.
6. Especifique quais dispositivos quer reparar. Se quiser que os dispositivos atuais afetados sejam adicionados automaticamente à lista alvo da janela Tarefas agendadas, selecione **Adicionar todos os dispositivos afetados**. Os dispositivos vulneráveis são aqueles onde a vulnerabilidade foi detectada pela última análise. Você também pode adicionar mais alvos depois de criada a tarefa na janela Tarefas agendadas.
7. Se quiser que os patches sejam distribuídos usando a Multidifusão dirigida, marque a caixa de seleção **Usar multidifusão**. Para configurar as opções de Multidifusão, clique no botão **Opções de multidifusão**. Para obter mais detalhes, consulte "Sobre a caixa de diálogo Opções de multidifusão" na página 640.
8. Se quiser usar a opção de download de parceiro unicamente para a distribuição de patches, marque a caixa de seleção **Fazer download de patch somente de parceiros locais**. Se você selecionar essa opção, o arquivo de patches será distribuído somente se ele residir no cache local do dispositivo ou em um parceiro da mesma sub-rede. Essa opção conserva a largura de banda da rede, mas observe que para a instalação da correção ser bem-sucedida, ela deve estar em um desses dois locais.
9. Especifique se quer somente descarregar o patch e não distribuir e instalá-lo nos dispositivos afetados.
10. Selecione uma configuração de análise e reparo para esta tarefa de reparo. As configurações de análise e reparo determinam a tela da análise, reinicialização e o comportamento da interação do usuário nos dispositivos analisados, assim como o conteúdo sendo analisado.
11. Clique em **OK**.
12. A tarefa aparece na janela Tarefas agendadas com o nome do trabalho especificado acima, onde você poderá personalizar a lista de dispositivos alvo e configurar as opções de agendamento.

Use uma diretiva de reparo (apenas no Windows)

A correção baseada em diretivas oferece flexibilidade permitindo atingir dispositivos alvo dinamicamente com base nos resultados de um LDAP personalizado ou de uma consulta ao banco de dados núcleo. Por exemplo, você pode configurar uma diretiva de correção de maneira que ela seja executada somente em dispositivos de um determinado contêiner de diretório ou somente em dispositivos que executem um determinado SO (ou em qualquer outro atributo de inventário que possa ser consultado). O Patch e conformidade usa diretivas nas Tarefas agendadas/ferramenta de distribuição de Software para configurar e processar as diretivas de correção.

NOTA: Plataformas suportadas para correção baseada em diretiva
Correção baseada em diretiva é suportada apenas nos dispositivos Windows. Os dispositivos Macintosh não podem ser corrigidos através do método de diretiva de aplicativo.

Para ser corrigido com base em uma diretiva, um dispositivo deve ter o agente de distribuição de Software instalado. Quando o agente é executado, ele verifica o banco de dados núcleo para encontrar diretivas que possam ser aplicadas ao mesmo. Se elas existirem, será exibida uma caixa de diálogo no dispositivo mostrando as diretivas recomendadas e opcionais (as diretivas necessárias são aplicadas automaticamente).

As diretivas de correção (ou reparo) operam de modo muito parecido com as diretivas de aplicativos, exceto que nesse caso são distribuídos arquivos de correções em vez de arquivos de aplicativos. Os pré-requisitos de gerenciamento de diretivas, fluxo de tarefas, tipos de diretivas e direcionamento estático e dinâmico são basicamente idênticos em ambos os casos.

Para criar uma correção baseada em diretivas

1. Clique em **Ferramentas > Patch e conformidade**.
2. Clique com o botão direito em uma única definição de um dos grupos de conteúdo ou clique com o botão direito em um grupo personalizado e clique em **Reparar**. Ou, clique no botão **Criar uma tarefa** da barra de ferramentas e clique em **Reparar**. A caixa de diálogo **Criar tarefa de reparo** é exibida.
3. Edite o **Nome da tarefa** se quiser mudar o nome da tarefa de reparo.
4. Marque a caixa de seleção **Reparar como uma diretiva**.
5. Se quiser criar uma nova consulta, baseada nesta definição de vulnerabilidade a qual poderá ser usada mais tarde para analisar outros dispositivos de gerenciamento, consulte a caixa de seleção **Adicionar consulta**.
6. Se quiser usar a opção de download de parceiro unicamente para a distribuição de patches, marque a caixa de seleção **Fazer download de patch somente de parceiros locais**. Se você selecionar essa opção, o arquivo de patches será distribuído somente se ele residir no cache local do dispositivo ou em um parceiro da mesma sub-rede. Essa opção conserva a largura de banda da rede, mas observe que para a instalação da correção ser bem-sucedida, ela deve estar em um desses dois locais.
7. Especifique se quer somente descarregar o patch e não distribuir e instalá-lo nos dispositivos afetados.
8. Selecione uma configuração de análise e reparo para esta diretiva de reparo. As configurações de análise e reparo determinam a tela da análise, reinicialização e o comportamento da interação do usuário nos dispositivos analisados, assim como o conteúdo sendo analisado.
9. Clique em **OK**.
10. A nova diretiva aparece no grupo Diretivas na janela Tarefas agendadas com o nome especificado acima. Nessa tela você pode adicionar alvos estáticos (usuários ou dispositivos) e alvos dinâmicos (resultados de consultas) e configurar o tipo e a freqüência da diretiva.

Use um Reparo automático

O Reparo automático é um conveniente método integrado para correções rápidas em casos nos quais não se deseja criar uma tarefa agendada ou uma tarefa de reparo baseada em diretivas. Por exemplo, se existir uma nova vulnerabilidade conhecida que você queira analisar e reparar em um único processo, poderá usar o recurso Reparo automático.

O Reparo automático está disponível para os seguintes tipos de conteúdo: vulnerabilidades, spyware, atualizações de software da LANDesk e definições personalizadas.

IMPORTANTE: Requisitos para uso do Reparo automático
Somente administradores ou usuários com direitos para o Patch Manager e para o escopo Padronizar todos os computadores podem habilitar o recurso Reparo automático para as definições aplicáveis. Os usuários LANDesk sem direitos de administrador do LANDesk ou para o Patch Manager não verão essa opção no menu de atalho (clique com o botão direito do mouse) de uma definição. Para obter mais informações sobre direitos e escopos, consulte "Gerenciamento de usuários" na página 38.

O Reparo automático deve estar habilitado em dois lugares para funcionar corretamente. Primeiro, a opção Reparo automático precisa ser ativado e, em segundo lugar, é necessário aplicar as configurações de análise e reparo à tarefa agendada de análise. Se uma opção de reparo automático de um desses itens NÃO estiver habilitada, o reparo automático não ocorrerá.

Quando o recurso Reparo automático for habilitado em ambos os lugares mencionados acima, na próxima vez que a análise de segurança for executada (manualmente ou por meio de uma tarefa de análise), o Patch e conformidade instala automaticamente o patch necessário em qualquer dispositivo afetado. Com a Correção automática, quando a reinicialização for necessária para uma correção, o dispositivo alvo sempre reinicializará automaticamente.

Você pode habilitar o Reparo automático para uma definição individual ou um grupo com várias seleções de definições de uma única vez.

Para configurar o Reparo automático baseado em diretivas

1. Na janela da ferramenta **Patch e conformidade**, clique com o botão direito em uma ou mais definições selecionadas de um dos grupos de conteúdo e, a seguir, clique em **Fazer reparo automático ao analisar**. (**NOTA:** Não é possível habilitar o reparo automático em um grupo personalizado.)
2. Execute a análise de segurança nos dispositivos que quiser analisar e corrigir automaticamente usando uma tarefa de análise de segurança agendada com uma configuração de análise e reparo onde a opção de reparo automático estiver habilitada.

Correção manual de dispositivos Linux e UNIX

Os dispositivos Windows e Macintosh podem ser corrigidos remotamente do console mas outras plataformas como Linux e UNIX Sun Solaris só podem ser analisadas através do console, e não corrigidas.

É necessário instalar manualmente os patches apropriados nos dispositivos Linux e UNIX a fim de corrigi-los.

O que acontece com o dispositivo durante a correção

A correção automática requer a distribuição e a instalação de patches em dispositivos gerenciados Windows, por meio de qualquer um dos três métodos descritos nas seções anteriores.

É importante lembrar que um trabalho de reparo pode incluir a correção de uma ou mais definições de segurança detectadas. Além disso, uma única definição detectada pode exigir a instalação de um ou mais patches. Devido a esses fatores, a correção pode implicar na instalação de apenas um ou vários arquivos de patches no dispositivo, dependendo do número e do tipo de detecções.

Quase todos os arquivos de patch são instalados de maneira silenciosa, que significa transparente, não exigindo nenhuma interação no dispositivo do usuário final. Algumas correções para Windows 9.x e correções de idiomas diferentes do inglês não são instaladas silenciosamente. É possível dizer se um patch é instalado silenciosamente ou não verificando a coluna Instalação silenciosa de uma listagem de patches. Para obter mais informações, veja "Entenda e use a Janela da ferramenta de Patch e conformidade" na página 555.

Configuração da tela de análise de segurança e interação nos dispositivos do usuário final

Porém, possa um arquivo patch, ser ou não instalado silenciosamente, agora você pode configurar a quantidade de exibição da análise de segurança e de aviso para entrada no dispositivo do usuário final com o recurso de configurações de análise e reparo.

NOTA: Reinicialização consolidada
Se uma instalação do arquivo patch requerer uma reinicialização (e a opção **Nunca reinicializar** não estiver selecionada na página Reinicializar das configurações de análise e reparo aplicada à tarefa em questão), o Patch e conformidade instala primeiro *todos* os patches da tarefa especificada no dispositivo e então reinicializa uma vez o dispositivo.

Comandos adicionais (somente para definições personalizadas)

A correção da definição personalizada pode incluir comandos adicionais especiais definidos na criação de uma regra de detecção personalizada. Os comandos adicionais são executados na ordem especificada naquela guia Comandos da regra e de acordo com os argumentos de cada comando. Comandos adicionais podem ser executados antes, durante ou depois da execução do arquivo de correção.

Exibir as informações de segurança e patch dos dispositivos analisados

Como mencionado anteriormente, uma maneira de ver os dados de segurança analisados é por dispositivo. Para fazê-lo, clique com o botão direito em um dispositivo único ou em um grupo de dispositivos selecionados, em seguida clique em **Informações de segurança e patch**.

Esta página fornece muitas funções úteis. Com um ou mais dispositivos selecionados, você pode:

- Ver as listas de definições detectadas
- Ver informações detalhadas sobre quando e porque ocorreu a detecção
- Ver os patches instalados e as listas de atualização de software
- Ver informações detalhadas sobre quando o patch foi instalado ou desinstalado
- Limpar o status de instalação do patch
- Ver os dados históricos de reparo
- Limpar os dados históricos de reparo

Você também pode clicar com o botão direito nas definições e regras de detecção nas respectivas listas de item para executar tarefas comuns para um ou mais dispositivos afetados.

Visualizar as datas de análise de segurança mais recentes no inventário do dispositivo

Para ver quando a última análise de segurança foi executada em um dispositivo, clique com o botão direito no dispositivo, clique em **Inventário** e, em seguida, role para baixo até **Últimas datas de análise** no painel direito da tela Inventário.

Verificar status de correção

Depois de realizar as correções nos dispositivos afetados, o Patch e conformidade cria relatórios sobre o status de cada instalação de patch. Você pode verificar o status das instalações de patches por vulnerabilidade/definição e por dispositivo alvo.

Para verificar a instalação do patch em um dispositivo

1. Execute o analisador de segurança no dispositivo.
2. Clique com o botão direito em um dispositivo corrigido na tela de rede e, em seguida, clique em **Informações de segurança e patch**.
3. Clique no objeto **Patches instalados** no painel esquerdo.
4. Selecione os campos de **Informações de patch** na parte inferior do diálogo.

O campo **Status da instalação** indica se a instalação foi bem sucedida. Os estados possíveis são: Bem-sucedida, Com falha e Falha de download.

Limpar a análise de vulnerabilidade e status do reparo por vulnerabilidade

Se houver uma falha na instalação de uma correção, você deverá primeiro limpar essas informações de status antes de tentar instalar novamente a correção. Você pode limpar o status da instalação (reparar) do dispositivo selecionado clicando em **Limpar**, na caixa de diálogo **Informações de segurança e patch**. Você também pode limpar o status de instalação do patch por vulnerabilidade.

Apague as informações de status de análise de vulnerabilidade e reparo para todos os dispositivos afetados por uma vulnerabilidade (ou vulnerabilidades utilizando a caixa de diálogo **Limpar status de análise/reparo**). Conforme explicado anteriormente, se houver uma falha na instalação de uma correção, você deverá primeiro limpar o status de instalação (reparo) antes de instalar novamente a correção.

Use também esta caixa de diálogo para remover as informações de análise de vulnerabilidade do banco de dados para uma ou mais vulnerabilidades.

Para limpar o status da análise de vulnerabilidade e reparo

1. Clique com o botão direito em vulnerabilidade e selecione **Limpar status da análise/reparo**.
2. Selecione as opções de filtro desejadas.
3. Slecione **Limpar**.

Criar uma tarefa de reinicialização agendada

O Patch e conformidade fornece uma ferramenta que permite a criação de uma tarefa de reinicialização do dispositivo. Uma tarefa de reinício pode ser útil quando quiser instalar patchs, sem reinicializar, como um processo único e então reinicializar outros dispositivos corrigidos como outra tarefa separada. Por exemplo, você pode executar uma análise ou uma instalação de patch durante o dia, e depois distribuir uma tarefa de apenas reinício quando for mais conveniente para os usuários finais.

Para criar uma tarefa de reinicialização

1. Clique em **Ferramentas > Patch e conformidade**.
2. Clique no botão **Criar uma tarefa** da barra de ferramentas e clique em **Reiniciar**.
3. Especifique se a reinicialização é uma tarefa agendada ou uma análise baseada em diretivas, ou ambas.

4. Selecione uma configuração de análise e reparo na lista disponível (ou crie uma configuração personalizada somente para esta análise) para especificar como a análise funciona nos dispositivos do usuário final. (**NOTA:** Somente as configurações de reinicialização nas definições de análise e reparo são usadas como tarefa de reinicialização.)
5. Clique em **OK**. Para uma tarefa agendada, agora você pode acrescentar dispositivos de origem e configurar as opções de agendamento na ferramenta Tarefas agendadas. Para uma diretiva, a nova diretiva aparece na janela Gerenciamento da diretiva do aplicativo com o nome da tarefa especificado acima, onde pode-se adicionar alvos estáticos (usuários ou dispositivos) e alvos dinâmicos (resultados da pesquisa) e configurar o tipo e a freqüência da diretiva.

Usar a linha de comando de análise de segurança

O LANDesk Security Suite inclui a ferramenta Patch e Conformidade como componente principal de sua solução abrangente de gerenciamento de segurança. Use esta ferramenta para baixar atualizações de várias definições e patches de tipo de conteúdo de segurança; criar, configurar e executar análises de avaliação, análises de conformidade e análises de correção; ativar alertas de segurança; gerar relatórios de segurança e muito mais. Para saber mais, consulte "Patch e conformidade" na página 549 e "Ajuda do Patch e conformidade" na página 620.

Este capítulo fornece informações suplementares sobre o uso da análise de segurança do Patch e Conformidade.

Parâmetros de linha de comandos do analisador de inventário

A análise de segurança é chamada vulscan.exe. O SDCLIENT.EXE é compatível com os seguintes parâmetros de linha de comandos:

Nome do parâmetro	Descrição
Parâmetros gerais	
/AgentBehavior=ScanRepairSettingsID	Sobregrava o comportamento padrão do analisador de segurança (configurações de análise e reparo) apenas para a tarefa de avaliação da segurança atual ou de análise de correção. O ID do ScanRepairSettings é um valor numérico.
/ChangeBehaviors /AgentBehavior=ScanRepairSettingsID	Muda as configurações padrão de análise e reparo para as tarefas subsequentes de avaliação de segurança e análise de correção, ao gravar as configurações de análise e reparo no registro local do dispositivo. Use a sintaxe exata à esquerda, com ambas as opções na linha de comando. O ID do ScanRepairSettings é um valor numérico. **NOTA:** Você pode usar esta opção para mudar as configurações padrão de análise e reparo dos dispositivos sem ter que distribuir uma configuração completa de agente para os dispositivos.

Nome do parâmetro	Descrição
/ShowUI	Exibe a IU (interface do usuário) do analisador no dispositivo de um usuário final.
/AllowUserCancelScan	Mostra um botão Cancelar na IU da análise, que permite o usuário final cancelar a análise.
/AutoCloseTimeout=Number	Valor do tempo limite em segundos. **NOTA:** Se o valor for definido em -1, a IU da análise aguarda o usuário final fechá-la manualmente.
/Scan=Number Code (0-8)	Identifica o tipo de conteúdo de segurança procurado pela análise. O número de códigos para tipos diferentes de conteúdo de segurança: 0 - vulnerabilidade 1 - spyware 2 - ameaça de segurança 3 - atualização da LANDesk 4 - definição personalizada 5 - aplicativo bloqueado 6 - atualizações de software 7 - atualizações de driver 8 - antivírus 100 - todos os tipos
/Group=GroupID	Identifica o grupo do conteúdo de segurança procurado pela análise. Essa opção cancela os parâmetros do tipo de conteúdo específico, se estiverem presente.
/AutoFix=True or False	Ativa ou desativa o recurso de reparo automático (autofix).
Parâmetros do reparo	
/Repair (Group=GroupID ou Vulnerability=VulnerabilityID ou Vulnerability=All)	Informa a análise qual grupo ou vulnerabilidade a reparar (corrigir). Você pode especificar Todas para vulnerabilidades a fim de reparar todas as vulnerabilidades detectadas por seu ID em vez de apenas uma vulnerabilidade.
/RemovePatch=PatchName	Remove o patch especificado do repositório de patchs.

Nome do parâmetro	Descrição
/RepairPrompt=MessageText	Permite mostrar uma mensagem de texto que avisa o usuário final.
/AllowUserCancelRepair	Uma string que permite ao usuário final cancelar o reparo se estiver usando um prompt de reparo.
/AutoRepairTimeout=Number	Um valor de tempo limite para o prompt de reparo em segundos. Se o valor for definido em -1, a IU aguarda que o usuário feche-a manualmente.
/DefaultRepairTimeoutAction	Uma string para a ação padrão a ser executada pelo vulscan se o tempo limite para o prompt estiver esgotado. Valores aceitáveis incluem iniciar e fechar.
/StageOnly	Uma string para obter o patch ou patches necessários para reparo, mas sem instalá-los.
/Local (obtém arquivos de parceiro)	Força o download de parceiro apenas.
/PeerDownload	O mesmo que /local.
/SadBandwidth=Number	Porcentagem máxima de largura de banda a usar durante o download:
Parâmetros de reinicialização	
/RebootIfNeeded	Use este parâmetro para reinicializar o computador se necessário.
/RebootAction	Uma string que determina o comportamento de reinicialização de vulscan ao fazer o reparo: Valores aceitáveis: sempre, nunca ou vazio (qualquer outro). Se qualquer outro, então a vulscan é reinicializada, se necessário.
/RebootMessage	Uma string que exibe uma mensagem de texto ao usuário no aviso de reinicialização.
/AllowUserCancelReboot	Uma string que permite que o usuário cancele o reparo se estiver usando um prompt de reparo.
/AutoRebootTimeout=Number	Valor de tempo limite do prompt de reinicialização, em segundos. Se o valor for definido em -1, a IU aguarda que o usuário feche-a manualmente.

Nome do parâmetro	Descrição
/DefaultRebootTimeoutAction	Uma string que determina a ação do vulscan se o tempo limite para o prompt de reinicialização estiver esgotado. Valores aceitáveis: reinicializar, fechar, adiar.
/SnoozeCount=Number	Número de adiamentos. O Vulscan diminui cada vez que o usuário clicar em **Adiar** no prompt de reinicialização.
/SnoozeInterval=Number	Número de segundos de repouso da vulscan entre atrasos.
Parâmetros de MSI	
/OriginalMSILocation=path	Caminho para o local original do MSI.
/Username=username	Nome do usuário para o diretório do MSI.
/Password=password	Senha para o diretório do MSI.
Desativar parâmetros	
/NoElevate	Não lançar a vulscan através da tec. do núcleo.
/NoSleep	Impede o repouso durante a análise de definição
/NoSync	Não obtém mutex, analisa múltiplas instâncias.
/NoUpdate	Não obtém uma nova versão da vulscan.
/NoXML	Não procure o msxml.
/NoRepair	O mesmo que autofix=false. Cancela as configurações de reparo automático se presente.
Parâmetros de arquivos de dados	
/Dump	Despeja dados de vulnerabilidade diretamente do serviço da Web.
/Data	Extrai dados de vulnerabilidade (de /dump).
/O=Path\Filename	Produz os resultados da análise.
/I=Path\Filename	Entra os resultados da análise.

Nome do parâmetro	Descrição
/Log=Path\Filename	Cancela o nome do arquivo de log.
/CoreServer=Server name	Identifica o nome do servidor núcleo.
/Reset	Remove as informações básicas do arquivo delta (limpa o diretório de dados do aplicativo).
/Clear ou /ClearScanStatus	Limpa todas as informações análise de vulnerabilidade.

Configurar alertas de patch e conformidade

A seguinte seção descreve outras tarefas que você pode executar com a ferramenta de Patch e conformidade.

Configurar alertas de patch e conformidade

Você pode configurar alertas de segurança de patch e conformidade de forma a ser notificado quando forem detectadas vulnerabilidades específicas em dispositivos gerenciados no seu sistema. Os alertas de vulnerabilidade de Patch e conformidade utiliza a ferramenta de alerta padrão LANDesk.

É necessário copiar uma vulnerabilidade para o grupo Alerta a fim de gerar um alerta quando houver detecção. A vulnerabilidade no grupo Alerta é uma cópia que também reside no grupo Analisar. Após colocar as definições de vulnerabilidade desejadas no grupo Alerta (manualmente ou especificando as vulnerabilidades de nível de gravidade para serem colocadas automaticamente durante downloads), você pode configurar o intervalo de alerta na caixa de diálogo Configurar alertas.

Para configurar alertas

1. Especifique as vulnerabilidades que gerarão alertas, colocando manualmente as definições de vulnerabilidade descarregadas no grupo Alerta.
2. Ou, clique no botão **Configurar definições**, em seguida, clique em **Configurações de alerta**.
3. Especifique um intervalo mínimo de alerta.
4. Para configurar alertas de segurança, selecione as definições (por nível de gravidade) que deseja colocar automaticamente no grupo **Alerta** durante o processo de download. Você pode selecionar mais de um nível de gravidade de vulnerabilidade. Essas definições de vulnerabilidade também serão colocadas automaticamente no grupo Analisar.
5. Se você quiser configurar alertas de antivírus, selecione os eventos de antivírus para os quais deseja gerar alertas.
6. Clique em **OK**.

Gerar relatórios de patch e conformidade

Informações de Patch e conformidade são representadas na ferramenta Relatórios. Esses relatórios fornecem informações úteis sobre avaliação de risco de segurança, conformidade, distribuição de patch e status de correção para dispositivos analisados na sua rede para cada um dos vários tipos de conteúdo de risco de segurança.

Para acessar a ferramenta Relatórios, gerar e exibir relatórios, o usuário precisa ter direitos de administrador LANDesk (o que implica direitos plenos) ou direitos específicos para a função de Relatórios.

Para obter mais informações sobre o uso da ferramenta Relatórios, consulte "Relatórios" na página 197.

Visão geral dos padrões FDCC de conformidade

O LANDesk Security Suite agora fornece suporte a análise de segurança estendida e remediação para a iniciativa do Federal Desktop Core Configuration (FDCC). Os produtos de software da LANDesk foram certificados pelo National Institute of Standards and Technology (NIST) em conformidade com os padrões Security Content Automation Protocol (SCAP) e estão listados como produtos validados no site do National Vulnerability Database.

Você pode implementar conformidade de padrões de FDCC em seu ambiente de rede da organização usando o Remendo e ferramentas de Conformidade e características para executar segurança escanear básico e tarefas de remediação com conteúdo de segurança de FDCC-CERTIFICOU (isto é, definições de vulnerabilidade). Com uma segurança subscrição contente que inclui este conteúdo de segurança de FDCC-CERTIFICOU DE LANDesk-PUBLICOU, você pode: detecta e instala a aplicação de scanner de segurança de FDCC; cheque para conformidade de segurança de FDCC; e vulnerabilidade de FDCC de corrida escaneando e remediação. Ao fazer isto, você assegura seus dispositivos administrados (clientes) cumprem com os padrões Federais de Configuração de Centro de área de trabalho e requisitos.

Capacidades validados de SCAP

A seguinte vulnerabilidade escaneando, gerência de remendo, e capacidades de remediação (como definido pelo Instituto Nacional de Padrões e a Tecnologia) foi validado para LANDesk Security Suite:

- **O Scanner de FDCC:** "; a capacidade de auditorar e de avaliar um sistema de alvo para determinar sua conformidade com os requisitos de FDCC. ";
- **Scanner autenticado de Configuração:** "A capacidade de auditorar e de avaliar um sistema alvo para determinar sua conformidade com um conjunto de requisitos de configurações definido usando privilégios de logon de sistema alvo. "
- **Vulnerabilidade autenticada e Remenda Scanner:** "; a capacidade de escanear um sistema de alvo para localizar e identificar a presença de vulnerabilidades sabidos, e avalia o estado de remendo de software para determinar conformidade com uma apólice definida de remendo usando privilégios de logon de sistema de alvo. "

Plataformas de dispositivo com suporte

Análise de vulnerabilidades certificada pela FDCC é suportado nas seguintes plataformas de dispositivos gerenciados (cliente):

- Microsoft Windows Vista SP1
- Microsoft Windows XP Professional SP3

Fazer o download do conteúdo específico de segurança do FDCC

This section provides step-by-step instructions for downloading the Federal Desktop Core Configuration (FDCC) security content.

IMPORTANTE: Remember that in order to download any security content, you must have a content

subscription. In this case, you must have a LANDesk Security Suite content subscription that specifically includes the FDCC content.

Exibir o conteúdo de segurança do FDCC

1. No console, clique em **Ferramentas > Segurança > Patch e conformidade**.
2. Clique no botão da barra de ferramentas **Fazer o download das atualizações**.
3. Selecione o site de origem das atualizações na lista de servidores de conteúdo disponíveis.
4. Selecione os tipos de definição cujo conteúdo de segurança que você quer atualizar. In this case, select **Federal Desktop Core Configuration** from the Definition types list. Você pode selecionar um ou mais tipos na lista dependendo da sua assinatura de conteúdo da LANDesk Security Suite. Quantos mais tipos você selecionar, maior será o tempo necessário para a atualização.
5. Selecione os idiomas cujo conteúdo você deseja atualizar para os tipos que especificar. In this case, select **English**.
6. Se você desejar que o novo conteúdo (conteúdo que já não seja residente em nenhum grupo da árvore) seja colocado automaticamente no grupo Não atribuído em vez de no local padrão, que é o grupo Analisar, selecione a caixa de seleção **Colocar as novas definições no grupo "Não designados"**.
7. Se quiser descarregar automaticamente os arquivos executáveis dos patches, selecione na caixa de seleção **Download de patches**, em seguida clique em uma das opções de download. (**NOTA:** Os patches são descarregados no local especificado na página Local do patch da caixa de diálogo Download de atualizações.)
8. Se tiver um servidor proxy na rede usado para transmissões externas da Internet (necessárias para atualizar o conteúdo de segurança e o download de patches), clique em **Configurações Proxy** e especifique o endereço do servidor, o número da porta e as credenciais de autenticação, se for necessário um login para acessar o servidor proxy.
9. Clique em **Aplicar** a qualquer momento para salvar as configurações.
10. Clique em **Atualizar agora** para executar a atualização de conteúdo de segurança. A caixa de diálogo Atualização de definições mostra a operação atual e o status.
11. Quando a atualização estiver concluída, clique em **Fechar**. Observe que se você clicar em **Cancelar** antes do término da atualização, somente o conteúdo de segurança que já foram processadas até este ponto são inseridas no banco de dados núcleo. Seria necessário executar a atualização novamente para obter o conteúdo de segurança restante.

After the FDCC content is downloaded, you can view and manage the content in order to perform compliance scans and remediation.

Exibir o conteúdo do download de segurança do FDCC

The FDCC content will be downloaded to the core server and a new Federal Desktop Core Configuration group will be created under the Predefined Groups parent object; with subgroups for supported OS platforms (Windows Vista, and Windows XP) as well as specific component checks. The component check subgroups include:

- Firewall
- Internet Explorer
- Correções
- Configurações

The downloaded FDCC vulnerability definitions are classified as Security Threats. In order to see the definitions, you must select either **Security Threats** or **All Types** in the Type drop-down list.

Instalar o analisador de segurança do FDCC

Esta seção descreve como verificar dispositivos administrados (clientes) para a agente/aplicação de scanner de segurança de FDCC, e instalam o scanner se for necessário.

Após fazer o download do conteúdo FDCC-ESPECÍFICO de segurança, você deve instalar a aplicação de scanner de FDCC em dispositivos administrados antes que você pode configurar e poder correr escaneamentos de avaliação de vulnerabilidade de FDCC.

Para instalar o scanner de FDCC em clientes, cria uma tarefa programada escanear e remediar o FDCC-SCANNER-INSTALA definição de vulnerabilidade. Esta definição pode ser achado no (Passo 1) Instala o subgrupo de Scanner sob o grupo Federal de Configuração de Centro de área de trabalho. Esta definição de ameaça de segurança verifica ver se o scanner de FDCC deve ser instalado em clientes de alvo. Se não acha a aplicação de scanner de FDCC no cliente, a remediação é instalar os diretórios necessários e arquivos. (**NOTA:** A aplicação de scanner de FDCC é instalada na seguinte localização: Program Files\LANDesk\LDClient\S-CAT.)

IMPORTANTE: Os Escritores de Manuscrito de LANDesk agrupam permissão é exigido executar estas tarefas. Para criar tarefas agendadas e diretivas na ferramenta Patch e conformidade e a ferramenta Configurações de segurança (para tarefas de análise de segurança e conformidade, tarefas de reparo e tarefas de mudanças de configurações), um usuário precisa ter permissão de grupo LANDesk Script Writers. Em outras palavras, eles precisam pertencer a um grupo que tenha permissão de LANDesk Script Writers atribuída. Para obter mais informações, consulte a Administração com base em funções no Guia do usuário.

Para criar uma tarefa programada de análise de segurança que instala o scanner de FDCC

1. No console, clique em **Ferramentas > Segurança > Patch e conformidade**.
2. Assegure-se que o conteúdo de segurança de FDCC foi atualizado recentemente.
3. Clique no botão **Criar uma tarefa** da barra de ferramentas e clique em **Análise de segurança**. A caixa de diálogo Criar tarefa de análise de segurança é mostrado.
4. Digite um nome para a análise.
5. Selecione o **Cria uma caixa programada de cheque de tarefa** .
6. Para criar uma configuração de análise e reparo que use as definições de ameças de segurança FDCC-ANALISADOR-INSTALAR encontrado no subgrupo Install Scanner como o conteúdo para da análise de segurança, clique em **Configurar** e na página **Opções de análise**.
7. Para especificar o que escanear para, clicar **o Grupo**. Clique o navega botão, e então seleciona o **(Passo 1) Instala o subgrupo de Scanner** sob o grupo Federal de Configuração de Centro de área de trabalho.
8. No outro análise e páginas de configurações de reparação, especifique outras opções de análise de segurança como desejado.
9. Clique em **Salvar** para gravar as configurações de análise e reparo que você aplicou nesta tarefa de análise.
10. No diálogo de tarefa de análise de Segurança, clique **BEM**. Para uma análise agendada da tarefa, agora você pode acrescentar dispositivos de origem e configurar as opções de agendamento na ferramenta Tarefas agendadas.

Quando você corre o análise com esta ameaça de segurança, qualquer dispositivo de alvo que não tem o scanner de FDCC já instalado receberão os arquivos necessários de aplicação, como determinado acima. A este ponto você está agora pronto para verificar para conformidade de FDCC, e corre escaneamentos de conteúdo de segurança reais FDCC-ESPECÍFICOS e remediação.

Verifique a conformidade do FDCC

Esta seção fornece informações sobre correr um análise de segurança em dispositivos de alvo que gera um relatório de conformidade de FDCC.

Uma vez a aplicação de scanner de FDCC é instalada em seus dispositivos administrados, você pode criar e poder correr outra tarefa programada de análise de segurança que usa a definição de ameaça de segurança de ComplianceResultsFile. Esta definição pode ser achado no (Passo 2) o subgrupo de Escaneamento de Arquivo de Resultados sob o grupo Federal de Configuração de Centro de área de trabalho, e gera os dados de relatório de FDCC. Se nenhuns dados de relatório é achado no cliente nem se os dados de relatório é mais velhos que os dias especificaram na variável personalizada, a definição de ameaça de segurança é detectada, querendo dizer o dispositivo não está em conformidade.

Para criar uma tarefa de análise de segurança que verifica para e gera dados de relatório de FDCC, segue os mesmos passos no **criar um procedimento programado de tarefa** de análise de segurança descrito acima, selecionando o (Passo 2) o subgrupo de análise de arquivo de Resultados como o grupo escanear para no análise e configurações de reparação.

Executar análises de segurança do FDCC

This section describes how to use FDCC-specific security content (vulnerability definitions) to scan for and remediate security risks on your managed devices.

Each FDCC subgroup contains security threat vulnerabilities for each of the following components:

- Firewall
- Internet Explorer
- Correções
- Configurações

You can use these vulnerability definitions to create scheduled scan tasks that check the Pass/Fail status for each of these FDCC security areas. These security threat vulnerabilities will show what is detected (i.e., failed) on target devices.

To create security scan tasks that check for component-specific FDCC security content, follow the same steps in the **To create a scheduled security scan task** procedure described above, selecting the appropriate component subgroup as the group to scan for in the scan and repair settings.

Exibir resultados da análise de segurança do FDCC

FDCC security scan results can be viewed from either the Security and Patch Manager Tool or from the Security and Patch Manager Information window.

If a vulnerability definition fails then it is shown as detected with a (1) in the Detected column. If a vulnerability definition passes then it is shown as a (0) in the Detected column.

NOTA: A vulnerability definition is also provided that reports any machines that fail to pass the overall

score required to meet the FDCC configuration standard.

Ajuda do Patch e conformidade

A janela da ferramenta Patch e conformidade (**Ferramentas > Segurança e Conformidade > Patch e conformidade**) é onde você executa a análise de segurança, correção e tarefas relacionadas. Você pode descarregar e gerenciar conteúdo de segurança, configurar a análise segurança e conformidade, configurar a correção, personalizar e aplicar as configurações da exibição/interação da análise de segurança e exibir as informações relativas à segurança dos dispositivos analisados.

A seção principal do "Patch e conformidade" na página 549 introduz esta ferramenta de gerenciamento de segurança. Nesta seção você verá informações de conteúdo de segurança , visão geral e instruções detalhadas sobre como usar todos os recursos da ferramenta, incluindo uma descrição de sua interface e funcionalidade, consulte "Entenda e use a Janela da ferramenta de Patch e conformidade" na página 555.

Esta seção contém a seguinte ajuda online a seguir que descrevem as caixas de diálogos de Patch e conformidade. Pela interface do console, esses tópicos de ajuda são acessados clicando no botão **Ajuda** em suas respectivas caixas de diálogo.

- "Ajuda da ferramenta de Patch e conformidade" na página 620
- "Ajuda de download de atualizações de conteúdo de segurança" na página 621
- "Ajuda das propriedades da definição" na página 625
- "Ajuda das propriedades da regra de detecção" na página 629
- "Ajuda de tarefas de Patch e conformidade" na página 637
- "Ajuda da configurações de Patch e conformidade" na página 643
- "Ajuda da barra de ferramentas de Patch e conformidade" na página 653

Ajuda da ferramenta de Patch e conformidade

Sobre a caixa de diálogo Seleção de colunas

Use esta caixa de diálogo para configurar colunas de dados para listas de itens na janela da ferramenta Patch e conformidade. Você decide quais colunas de dados são mostradas para facilitar a ordenação em listas compridas de definições descarregadas de segurança e rápida e facilmente encontrar as informações necessárias para uma tarefa ou situação específica.

NOTA: Uso da coluna de dados ID CVE
A LANDesk Security Suite suporta a convenção de nomes CVE (Common Vulnerabilities and Exposures). Com o Patch e Conformidade você pode procurar vulnerabilidades por nomes CVE e ver as informações CVE das definições de vulnerabilidades das quais foi feito download. Para obter mais informações sobre a convenção de nomes CVE, compatibilidade da LANDesk com o padrão CVE e saber como usar a identificação CVE para encontrar vulnerabilidades individuais em Patch e conformidade, consulte "Procurar vulnerabilidades por seus nomes CVE" na página 576.

Ao adicionar e remover colunas de dados e movê-las para cima e para baixo na lista (à esquerda e à direita na tela da coluna), as informações relevantes e importantes são mostradas na parte superior e centrais.

- **Colunas disponíveis:** Mostra as colunas de dados não mostradas no momento na janela da ferramenta Patch e Conformidade, mas que estão disponíveis para serem adicionadas à lista Colunas selecionadas.
- **Colunas selecionadas:** Lista as colunas de dados exibidas na janela do Patch e conformidade. As colunas de dados são exibidas em uma lista descarregada de definições de segurança da esquerda para a direita na mesma ordem que são mostradas aqui de cima para baixo.
- **Padrões:** Restaura o padrão mostrado nas colunas de dados.

Sobre a caixa de diálogo Gerenciar filtros

Use esta caixa de diálogo para gerenciar filtros usados para personalizar o conteúdo de segurança exibido na lista de itens da janela do Patch e conformidade. Você pode usar filtros para facilitar uma lista muito comprida.

- **Novo:** Abre a caixa de diálogo Propriedades do filtro onde você pode definir as configurações do novo filtro.
- **Editar:** Abre a caixa de diálogo Propriedades do filtro onde você pode modificar e salvar o filtro selecionado.
- **Excluir:** remove permanentemente o filtro selecionado do banco de dados.
- **Use o filtro:** aplica o filtro selecionado à lista atual de itens. O filtro aplicado persiste quando você clica em diferentes grupos na exibição da árvore.

Sobre a caixa de diálogo Propriedades do filtro

Use essa caixa de diálogo para criar ou editar filtros de conteúdo da lista de segurança. Você pode filtrar por sistemas operacionais, gravidade do risco de segurança ou qualquer combinação de ambos.

- **Filtrar por nome:** identifica o filtro com um nome exclusivo. Esse nome é exibido na lista suspensa Filtro.
- **Filtrar sistemas operacionais:** especifica os sistemas operacionais cujas definições você deseja exibir nas listas de itens. Somente os itens associados aos sistemas operacionais que você selecionar são mostrados.
- **Filtrar por gravidade:** especifica as severidades cujas definições você deseja exibir nas listas de itens. Somente os itens cuja gravidade coincidem com os que você selecionou são mostrados.

Ajuda de download de atualizações de conteúdo de segurança

Sobre as caixas de diálogo Download das atualizações

Use esta caixa de diálogo para definir as configurações de download das atualizações de conteúdo de segurança, servidor proxy, local de download de patches, correção automática de spyware e as atualizações de antivírus e backup.

Após especificar os tipos de atualizações de conteúdo dos quais deseja fazer download e as outras opções nas páginas da caixa de diálogo Fazer o download das atualizações:

- Para fazer um download imediato, clique em **Fazer download agora**. Se você clicar em **Aplicar**, as configurações especificadas serão salvas e exibidas na próxima vez em que você abrir essa caixa de diálogo. Você deverá confirmar se deseja salvar as configurações ao clicar em **Fechar**.

- Para agendar uma tarefa de download de conteúdo de segurança, clique em **Agendar download** para abrir a caixa de diálogo **Informações de atualização agendada**, digite um nome para a tarefa, verifique as informações da tarefa e clique em **OK** para adicionar a tarefa às Tarefas agendadas.
- Você pode clicar em **Exibir log** para abrir o arquivo de log.

Para salvar as mudanças em qualquer página desta caixa de diálogo, clique em **Aplicar**.

A caixa de diálogo **Download de atualizações** contém as seguintes páginas:

- "Sobre a página Atualizações" na página 622
- "Sobre a página Configurações do proxy" na página 624
- "Sobre a página Local do patch" na página 625
- "Sobre a página LANDesk Antivirus" na página 625
- "Sobre a página Conteúdo" na página 625
- "Sobre a página Importar / Exportar" na página 625

IMPORTANTE: Considerações especiais sobre o download de conteúdo de segurança

Assinaturas de conteúdo do Security Suite

Uma instalação básica do LANDesk Management Suite permite o download e a análise de atualizações de software LANDesk e a criação e uso das suas definições personalizadas. Para todos os outros tipos de conteúdo de segurança, como vulnerabilidades específicas de plataformas, spywares etc, você deverá ter uma assinatura de conteúdo do LANDesk Security Suite para fazer download das definições associadas.

Para obter informações sobre assinaturas de conteúdo do Security Suite, entre em contato com o representante ou visite o site da LANDesk:

LANDesk Home

Configurações de tarefas específicas e globais

Observe que somente os tipos de definição, idiomas e configurações de download de definições e patches são salvos e associados quando você cria uma tarefa específica. Essas três definições são consideradas específicas a tarefas.

Entretanto, todas as definições nas outras páginas do diálogo Fazer o download das atualizações são globais, o que significa que se aplicam a todas as tarefas subseqüentes de download de conteúdo de segurança. As configurações globais de download do patch, servidor proxy, correção automática de spyware, alertas de segurança e antivírus. Quando você mudar configurações globais, ela estará em efeito para todas as tarefas de download de conteúdo de segurança daquele ponto em diante.

Sobre a página Atualizações

- **Selecionar o site da fonte da atualização:** Especifica o servidor de conteúdo da LANDesk acessado para fazer o download das últimas definições, regras de detecção e patches associados ao seu banco de dados. Selecione o servidor mais próximo do local onde você se encontra.

- **Tipos de definição:** Identifica as definições de conteúdo de segurança a serem atualizadas. Só estão disponíveis os tipos de definição aos quais você tem uma assinatura. Quanto mais tipos de definições você selecionar, maior será o tempo necessário para o download.

  Após o download do conteúdo de segurança você poderá selecionar a lista suspensa **Tipo** na janela principal da ferramenta Patch e Conformidade para determinar os tipos de definição exibidos em uma lista. Para obter informações sobre o uso das opções da lista, consulte "Lista suspensa Tipo" na página 558.

- **Idiomas:** determina as versões de idioma dos tipos de definição selecionados que serão atualizados.

  Alguns tipos de vulnerabilidades e de outras definições, assim como patches associados, têm idioma neutro ou independem do idioma, o que significa que são compatíveis com qualquer versão de idioma do SO ou do aplicativo considerado pela definição. Em outras palavras, não é necessário separar um patch com idioma específico para corrigir essas vulnerabilidades, uma vez que ela abrange todos os idiomas suportados. Por exemplo, as plataformas Linux e UNIX usam somente definições e patches neutros ao idioma. As definições de vulnerabilidade de plataforma do Microsoft Windows e Apple Macintosh, porém, são quase sempre específicas ao idioma.

  Ao fazer download do conteúdo de qualquer plataforma (com a assinatura apropriada de conteúdo de segurança), todas as definições neutras ao idioma da vulnerabilidade são atualizadas automaticamente, por padrão. Se selecionou o tipo de conteúdo Windows ou Mac, você deverá também selecionar os idiomas específicos cujas definições deseja atualizar. Se selecionou a plataforma Sun Solaris ou Linux, não é necessário selecionar um idioma específico, já que o conteúdo é neutro ao idioma e será atualizado automaticamente.

- **Download dos patches para as definições selecionados acima:** faz download automaticamente de arquivos executáveis de patch para o local de download especificado (veja a página Local do patch), de acordo com uma das seguintes opções de download:
  - **Para definições detectadas somente:** Faz download somente dos patches associados às vulnerabilidades, ameaças de segurança ou atualizações da LANDesk detectadas pela última análise de segurança (isto é, as definições que atualmente residem no grupo Detectadas).
  - **Para todas as definições descarregadas:** Faz download de TODOS os patches associados às vulnerabilidades, ameaças de segurança e atualizações de software da LANDesk atualmente no grupo Analisar.
- **Ativar a distribuição automática de patch usando o :** Vamos configurar o banco de dados do LANDesk Process Manager necessário para uso do recurso distribuição automática de patch.
- **LANDesk Process Manager** Clique no botão para abrir a caixa de diálogo Distribuição automática de patch que descreve a capacidade integrada entre o LANDesk Process Manager e a ferramenta Patch e conformidade que permite que você crie um fluxo de trabalho para automatizar a distribuição de patches para os dispositivos alvo. Você também possui a opção de visualização de um tutorial que o guia para executar esse procedimento. O Gerenciador de processos da LANDesk inclui tópicos de ajuda que pode ser acessada a qualquer hora para obter informações detalhadas sobre seus recursos e como usá-los.

- **Inserir novas definições em um grupo Não atribuído (a menos que seja sobrescrito por configurações do grupo de definições):** insere automaticamente novas definições e regras de detecção associadas no grupo Não atribuídas em vez de no grupo padrão Analisar. Selecione esta opção se desejar mover manualmente o conteúdo de e para o grupo Analisar para personalizada a análise de segurança.

  NOTA: As definições que têm dependência de outra definição que existe em um grupo diferente, como o grupo Analisar ou Não analisar, são colocadas automaticamente nesse grupo mesmo se essa opção estiver selecionada. Em outras palavras, a relação de dependência cancela esta opção para que a definição descarregada mais recentemente (nova) esteja no mesmo grupo da definição da qual ela tem dependência.

  NOTA: As definições que já tiverem sido selecionadas para serem colocadas no grupo Alertar (na caixa de diálogo **Configurar alertas**), são colocadas automaticamente no grupo Analisar mesmo se essa opção estiver selecionada, para que o alerta adequado ocorra).

  NOTA: Para o tipo de aplicativo bloqueado, o local padrão de download é diferente. As definições de aplicativo bloqueado são descarregadas para o grupo Não atribuída por padrão, e não para o grupo Analisar. Portanto, não é preciso seleciona esta opção se estiver descarregando apenas definições bloqueadas.

- **Configurações de grupo de definições:** Abre a caixa de diálogo Configurações de grupo de definições onde você pode criar, gerenciar e selecionar grupos de definição. É possível usar as configurações de grupos de definição para automatizar como o conteúdo de segurança (conteúdo), compatível com os critérios de severidade e tipo especificados, sejam obtidos por download, seu status de análise e o local de download.

Sobre a página Configurações do proxy

Se sua rede usa um servidor proxy para transmissões externas (como acesso à Internet), use essa página para habilitar e definir as configurações do servidor proxy. Acesso à Internet é necessário para atualizar informações de vulnerabilidades e para o download de arquivos de patches dos serviços apropriados da Web.

- **Usar servidor proxy:** Habilita a opção de servidor proxy (por padrão, essa opção é desativada). Se você habilitar um servidor proxy, deverá preencher os campos de endereço e porta abaixo.
- **Servidor:**
  - **Endereço:** Identifica o endereço IP do servidor proxy.
  - **Porta:** Identifica o número de porta do servidor proxy.
- **Proxy baseado em HTTP:** Habilita o servidor proxy, se for baseado em HTTP (como o Squid) para que a conexão e o download dos patches de sites FTP sejam bem-sucedidos. (Os patches baseados em alguns sites FTP não podem ser carregados através de um proxy baseado em HTTP a não ser que esta opção seja habilitada primeiro).
- **Requer login:** Permite digitar um nome de usuário e uma senha se o servidor proxy usa credenciais em vez de ser um servidor proxy transparente.
  - **Nome de usuário:** Digite um nome de usuário válido com credenciais de autenticação para o servidor proxy.
  - **Senha:** Digite a senha do usuário.

Sobre a página Local do patch

Use essa página para especificar onde são descarregados os executáveis de patch.

- **Caminho UNC onde os patches estão armazenados:** Especifica o local para download dos arquivos de patches. O local padrão é a pasta \LDLogon\Patch do servidor núcleo. Você pode digitar um outro caminho UNC para fazer download dos arquivos, mas deve garantir o acesso a esse local digitando credenciais de autenticação válidas nos campos abaixo.
- **Credenciais para armazenar patches:** Identifica um nome de usuário e uma senha válidos para acessar um local diferente do servidor núcleo. Se estiver descarregando patches para o local padrão no servidor núcleo, os campos nome do usuário e senha não são aplicáveis.
- **URL da Web onde os clientes acessam patches:** Especifica um endereço da Web onde os dispositivos podem acessar os patches obtidos por download para distribuição. O local padrão é a pasta \LDLogon\Patch do servidor núcleo. Normalmente, esse local é o mesmo que o caminho UNC especificado acima.
- **Testar configurações:** Executa um teste de conectividade com a URL da Web especificada.
- **Redefinir para o padrão:** Restaura o caminho UNC e o URL da Web para o local padrão, que é a pasta \LDLogon\Patch do servidor núcleo.

Sobre a página LANDesk Antivirus

Use esta página para configurar as opções de download para arquivos de definição de vírus do LANDesk Antivirus. Lembre-se de que essa página só se aplica a arquivos de definição de vírus usados pelo LANDesk Antivirus; ela não se aplica a conteúdo de detecção de análise antivírus (atualização de antivírus) disponíveis na lista de definição na página **Atualizações**.

Para obter informações detalhadas, consulte "Sobre a página LANDesk Antivirus na caixa de diálogo Download das atualizações" na página 736.

Sobre a página Conteúdo

Use essa página para...

- **Verificar assinaturas/hashs antes de fazer o download**

Sobre a página Importar / Exportar

Use esta página para configurar as configurações de importação ou exportação de antivírus.

- **Importar configurações do arquivo:**
- **Exportar configurações para arquivo:**
- **Copiar configurações para outro núcleo:**

Ajuda das propriedades da definição

Sobre a caixa de diálogo Propriedades da definição

Use essa caixa de diálogo para exibir as propriedades para tipos de definição de conteúdo baixado, inclusive vulnerabilidades, spyware, ameaças de segurança, atualizações de software, etc.

Você também usa esta página para criar suas próprias definições personalizadas.

Essas informações são somente para leitura nas definições descarregadas. Os campos nesta caixa de diálogo são editáveis para as definições personalizadas. Você pode inserir informações de identificação, atributo e detalhes da regra de detecção para uma definição personalizada usando os campos disponíveis nesta caixa de diálogo e também na de propriedades de regra de detecção.

Use os botões de seta para a direita e para a esquerda (<, >) para exibir informações de propriedade da definição anterior ou da próxima definição na ordem em que elas se encontram na janela principal.

A caixa de diálogo Propriedades da definição contém as seguintes páginas:

- "Sobre a definição: Página geral" na página 626
- "Sobre a definição: Página de descrição" na página 627
- "Sobre a definição: Página de dependências" na página 627
- "Sobre a definição: Página Variáveis" na página 627

Sobre a definição: Página geral

- **ID:** Identifica a definição selecionada com um código único, alfanumérico definido pelo fornecedor (ou definido pelo usuário no caso de uma definição personalizada).
- **Tipo:** Identifica o item selecionado como vulnerabilidade, ameaça de segurança, definição personalizada, etc.
- **Data de publicação:** Indica a data em que a definição selecionada foi publicada pelo fornecedor (ou criada por um usuário).
- **Título:** Descreve a natureza ou o destino da definição selecionada em um texto resumido.
- **Gravidade:** Indica o nível de severidade da definição. Para conteúdo descarregado, este nível de gravidade é designado pelo fornecedor. Para uma definição personalizada, a gravidade é atribuída por quem tiver criado a definição. Os níveis possíveis de gravidade são: Service Pack, Crítica, Alta, Média, Baixa, Não aplicável (N/A) e Desconhecida. Use estas informações para avaliar o risco colocado pela definição e a urgência da análise e correções para a sua rede.
- **Status:** Indica o status da definição na janela do Patch e Conformidade. Os três indicadores de status são: Analisar, significando que o item selecionado será habilitado na próxima análise de segurança; Não analisar, significando que ela não será analisada; e Não atribuídas, significando que ela não será analisada e que está temporariamente em uma área de armazenamento. Para obter mais informações sobre esses três estados/grupos, consulte "Entenda e use a Janela da ferramenta de Patch e conformidade" na página 555.
- **Idioma:** Indica o idioma da plataforma identificada pela definição. Para definições personalizadas, INTL é o valor padrão, significando que a definição é independente do idioma e não pode ser editada.
- **Categoria:** Indica uma categoria mais específica dentro de um tipo de conteúdo de segurança individual (veja acima).
- **Regras de detecção:** Lista as regras de detecção associadas à definição selecionada. Observe que a opção **Download** indica se o download dos arquivos de patch associados deverá ser feito no repositório local, e a opção **Instalação silenciosa** indica se o patch será instalado sem interação do usuário.

Clique no botão direito em uma regra de detecção para fazer download de seu patch (ou patches) correspondente, desabilitar/habilitar a regra de detecção para a análise de segurança, desinstalar patches associados ou ver suas propriedades. Clique duas vezes em uma regra de detecção para ver as suas propriedades.

Se estiver trabalhando com uma definição personalizada, clique em **Adicionar** para criar uma nova regra de detecção; clique em **Editar** para modificar a regra selecionada ou clique em **Excluir** para remover a regra selecionada.

Sobre a definição: Página de descrição

- **Descrição:** Fornece detalhes adicionais sobre a definição selecionada. Estas informações são apresentadas pelas notas de pesquisa e teste do fornecedor (ou pelo usuário que criou a definição personalizada).
- **Mais informações em:** Fornece um link HTTP com uma página da Web específica do fornecedor (ou definida pelo usuário), normalmente um site de suporte, com mais informações sobre a definição selecionada.
- **Mais informações para o ID CVE:** (Aplica-se somente a vulnerabilidades) Fornece o ID CVE (nome) para a vulnerabilidade selecionada, mais um link à página da Web do CVE para o ID CVE específico. Para obter mais informações, consulte "Procurar vulnerabilidades por seus nomes CVE" na página 576.

Sobre a definição: Página de dependências

Essa página mostra apenas se a definição selecionada tem uma definição de pré-requisito associada ou se outra definição depende da definição selecionada antes de poder ser executada. Use essa página para verificar se a sua tarefa de análise de segurança contém todas as definições necessárias para operar corretamente antes da análise dos dispositivos.

A relação de dependência só pode existir para os seguintes tipos de definição de segurança:

- **Pré-requisitos:** Lista as definições que devem ser executadas ANTES da definição selecionada poder ser verificada nos dispositivos. Se uma das definições nessa lista não estiver inclusa na sua tarefa de análise, a definição selecionada não será detectada pela análise de segurança.
- **Dependências:** Lista as definições que não serão detectadas pela análise de segurança até APÓS a definição selecionada ser executada. Observe que a definição selecionada será analisada mesmo se essas definições não forem incluídas na sua tarefa de análise de segurança. Entretanto, se desejar que a tarefa de análise detecte, com êxito, uma definição nessa lista, a definição selecionada deve ser executada primeiro.

Sobre a definição: Página Variáveis

Essa páginamostra SOMENTE se a definição de segurança selecionada inclui configurações ou valores que podem ser modificados. Algumas definições de ameaça de segurança de configuração de sistema têm parâmetros que foram mudados antes de incluí-las na análise de segurança. Normalmente, as definições de antivírus têm também configurações variáveis personalizadas.

Com as variáveis personalizadas é possível ajustar a análise de ameaça de segurança modificando um ou mais valores para que o analisador verifique as condições definidas e determine um dispositivo para ser vulnerável somente se aquela condição for satisfeita (por exemplo, o valor especificado é detectado).

IMPORTANTE: É necessário editar o direito Variáveis personalizadas
Para editar as configurações de variáveis personalizadas, o usuário LANDesk deve ter o direito de administração com base em função Editar variáveis personalizadas. Os direitos são configurados com a ferramenta **Usuários**.

Cada definição de segurança com variáveis personalizadas tem um conjunto exclusivo de valores específicos que podem ser modificados. Entretanto, em cada caso, a página **Variáveis personalizadas** mostrará as seguintes informações comuns:

- **Nome:** Identifica a variável personalizada. O nome não pode ser modificado.
- **Valor:** Indica o valor atual da variável personalizada. A menos que a variável seja de apenas leitura, você pode clicar duas vezes nesse campo para mudar o valor.
- **Adicionar variável:** Abra uma caixa de diálogo onde você pode criar sua própria variável personalizada. (NOTA: Antes que você possa criar uma variável personalizada para uma definição de vulnerabilidade personalizada, a definição deve primeiro conter ao menos uma regra de detecção.)
- **Editar variável:** Permite editar a variável personalizada selecionada.
- **Remover variável:** Exclui a variável personalizada selecionada.
- **Descrição:** Fornece mais informações úteis sobre a variável personalizada do editor de definição.
- **Valor padrão:** Fornece o valor padrão se você o mudou e deseja restaurá-lo ao valor original.

Para alterar uma variável personalizada, clique duas vezes no campo **Valor** e selecione um valor se houver uma lista suspensa disponível ou edite manualmente o valor, e clique em **Aplicar**. Observe que algumas variáveis são apenas leitura e não podem ser editadas (normalmente indicado na descrição).

As informações das configurações de substituição de variáveis personalizadas são exibidas no Inventário do dispositivo.

NOTA: Configurações de variáveis personalizadas a serem substituídas
Em algumas situações, talvez seja necessário ignorar as configurações de variável personalizada ou, em outras palavras, criar uma exceção à regra. É possível fazer isso com o recurso de configurações de substituição de variáveis personalizadas. As configurações para substituir as variáveis personalizadas permitem decidir quais variáveis deverão ser ignoradas ao analisar dispositivos para que eles não sejam detectados como vulneráveis e corrigidos mesmo que atendam às condições de regras de detecção de uma definição. Você pode criar quantas definições desejar e aplicá-las aos dispositivos usando uma tarefa **Mudar configurações**. Para obter mais informações, consulte "Sobre a caixa de diálogo Configurar as definições da variável personalizada a ser substituída" na página 650.

Sobre a caixa de diálogo Adicionar/editar variável personalizada.

Use esta caixa de diálogo para criar e editar as variáveis personalizadas para suas definições personalizadas de vulnerabilidade. Com as variáveis personalizadas é possível ajustar a análise de ameaça de segurança modificando um ou mais valores para que o analisador verifique as condições definidas e determine um dispositivo para ser vulnerável somente se aquela condição for satisfeita (por exemplo, o valor especificado é detectado).

IMPORTANTE: Antes que você possa criar uma variável personalizada para uma definição de vulnerabilidade personalizada, a definição deve primeiro conter ao menos uma regra de detecção.

Esta caixa de diálogo contém as seguintes opções:

- **Nome:** Identifica a variável personalizada.
- **Descrição:** Permite que você forneça informações adicionais úteis sobre a variável personalizada.
- **Tipo:** Identifica o tipo de recurso usado para definir a variável personalizada (inclusive: string, string criptografada, strings de multi-valor, número inteiro, enumeração, booleano).

- **Valores possíveis:** Insira todos os valores possíveis que podem ser considerados válidos para a variável personalizada sendo criadas (baseado no tipo acima especificado).
- **Valor padrão:** Insira o valor padrão da variável personalizada.

Ajuda das propriedades da regra de detecção

Sobre a caixa de diálogo Propriedades da regra de detecção

Use esta caixa de diálogo para exibir as propriedades da regra de detecção para conteúdo de segurança baixado ou para criar e editar regras de detecção personalizadas.

Estas informações são somente leitura para as regras de detecção que pertencem às definições descarregadas. Os campos nas páginas desta caixa de diálogo são editáveis para as definições personalizadas. Você pode especificar as configurações da regra de detecção e configurar as opções em cada página para criar regras de detecção personalizadas. Além disso, se a regra de detecção personalizada permitir correção, você pode adicionar comandos especiais que são executados durante o conserto (instalação ou desinstalação do patch).

Você pode usar os botões de seta para a direita e para a esquerda (<, >) para ver as informações de propriedade da regra de detecção anterior ou seguinte na ordem em que se encontram na janela principal.

A caixa de diálogo Propriedades da regra de detecção contém as seguintes páginas:

- "Sobre a Regra de detecção: Página geral de informações" na página 629
- "Sobre a Lógica de detecção: Páginas de plataformas afetadas" na página 630
- "Sobre a Lógica de detecção: Página de produtos afetados" na página 630
- "Sobre a Lógica de detecção: Arquivos usados para a página de detecção" na página 630
- "Sobre a Lógica de detecção: Configurações do registro usadas para a página de detecção" na página 631
- "Sobre a Lógica de detecção: Página de Script personalizado" na página 632
- "Sobre a página Informações do patch" na página 633
- "Sobre a Detecção do patch: Arquivos usados para a página de detecção de patch instalado" na página 634
- "Sobre a Detecção do patch: Configurações do registro usadas para a página de detecção de patch instalado" na página 634
- "Sobre a página Comandos de instalação do patch" na página 634
- "Sobre a página Comandos de desinstalação do patch" na página 636

Sobre a Regra de detecção: Página geral de informações

- **Nome:** Exibe o nome da regra de detecção.
- **Estado:** Indica se a regra de detecção está configurada para analisar ou não. Esses dois estados correspondem aos grupos Analisar e Não analisar (sob as Regras de detecção na janela do Patch e Conformidade).
- **ID:** Mostra a ID da definição associada a esta regra.
- **Título:** Mostra o título da definição ao qual esta regra está associada.
- **Descrição:** Mostra a descrição da definição ao qual esta regra está associada.

- **Comentários:** Apresenta informações adicionais do fornecedor do patch, se disponíveis. Se estiver criando ou editando uma definição personalizada, poderá inserir os seus comentários.

Páginas Lógica de detecção

As seguintes páginas referem-se à lógica de detecção usada pela regra de detecção selecionada para determinar se a definição de vulnerabilidade (ou outro tipo de definição) existe no dispositivo analisado.

Sobre a Lógica de detecção: Páginas de plataformas afetadas

Identifica os sistemas operacionais nos quais a varredura de segurança será executada para a definição associada desta regra. Em outras palavras, somente os dispositivos que coincidem com as plataformas selecionadas tentarão processar esta regra. Pelo menos uma plataforma DEVE ser selecionada. A análise de segurança é interrompida se o dispositivo alvo está sendo executado em um sistema operacional diferente.

Sobre a Lógica de detecção: Página de produtos afetados

- **Produtos:** Lista os produtos que deseja verificar com a regra de detecção para determinar se a definição associada existe nos dispositivos analisados. Selecione um produto na lista para ver seu nome, fornecedor e informações da versão. Não é necessária a associação de um produto com uma regra de detecção. Os produtos associados agem como um filtro durante o processo de análise de segurança. Se nenhum dos produtos associados específicos for encontrado no dispositivo, a análise de segurança é interrompida. Se nenhum produto for especificado, a análise continua com a verificação de arquivos.

Se você estiver criando ou editando uma regra de detecção personalizada, clique em **Configurar** para abrir uma nova caixa de diálogo para adicionar e remover produtos da lista. A lista de produtos disponíveis é determinada pelo conteúdo de segurança que você enviou através do serviço da Web da LANDesk Security Suite.

- **Nome:** Fornece o nome do produto selecionado.
- **Fornecedor:** Apresenta o nome do fornecedor.
- **Versão:** Fornece o número de versão do produto selecionado.

Sobre a Lógica de detecção: Arquivos usados para a página de detecção

- **Arquivos:** Lista as condições do arquivo (existência, versão, data, tamanho, etc) usadas para determinar se a definição associada existe nos dispositivos analisados. Selecione um arquivo na lista para ver o seu método de verificação e os parâmetros esperados. Se todas as condições do arquivo forem satisfeitas, o dispositivo não é afetado. Em outras palavras, se NENHUMA dessas condições forem satisfeitas, a vulnerabilidade existirá naquele dispositivo. Se não houver condições de arquivos na lista, a análise continua com a verificação do registro.
  Se estiver criando ou editando uma regra de detecção personalizada, clique em **Adicionar** para que os campos sejam editáveis, permitindo a configuração de uma nova condição de arquivo e valores/parâmetros necessários. As regras podem incluir uma ou mais condições de arquivo, dependendo da complexidade desejada. Para salvar uma condição de arquivo, clique em **Atualizar**. Para apagar uma condição de arquivo na lista, selecione-a e clique em **Remover**.
- **Verificar usando:** Indica o método usado para verificar se a condição de arquivos prescrita é atendida nos dispositivos analisados. Por exemplo, uma regra de detecção pode analisar a existência, versão, data, tamanho, etc. do arquivo. Os parâmetros esperados que são exibidos abaixo do método de verificação são determinados pelo próprio método (consulte a lista abaixo).

  Se você estiver criando ou editando uma regra de detecção personalizada, selecione o método

de verificação da lista suspensa **Verificar usando**. Assim sendo, os campos de parâmetro são diferentes para cada método de verificação, conforme a descrição na lista a seguir:

Observe que a opção **Procurar arquivo recursivamente** se aplica a todos os métodos de verificação de arquivos com exceção dos métodos MSI e faz com que a análise procure arquivos no local do caminho especificado e nas subpastas existentes.

- **Somente a existência do arquivo:** Verifica através da análise do arquivo especificado. Os parâmetros são: Caminho (local do arquivo no disco rígido), inclusive o nome do arquivo e Requisito (deve existir ou não deve existir).
- **Versão do arquivo:** Verifica pela análise do arquivo especificado e do seu número de versão. Os parâmetros são: Caminho, Versão mínima e Requisito (deve existir, não deve existir ou pode existir).

Observe que para os parâmetros de arquivo Versão, Data e Tamanho, você pode clicar no botão **Coletar dados** para preencher automaticamente os campos de valores apropriados.

- **Data do arquivo:** Verifica pela análise do arquivo especificado e de sua data. Os parâmetros são: Caminho, Data mínima e Requisito (deve existir, não deve existir ou pode existir).
- **Tamanho do arquivo e/ou soma de comprovação:** Verifica pela análise do arquivo especificado e de seu tamanho ou valor da soma de comprovação. Os parâmetros são: Caminho, Soma de comprovação, Tamanho do arquivo e Exigência (deve existir, não deve existir ou pode existir).
- **O ID de produto MSI está instalado:** Verifica se o produto MSI especificado está instalado (produto instalado pelo utilitário Microsoft Installer). Os parâmetros são: Guid (global unique identifier, ou o identificador único global do produto).
- **O ID de produto no MSI NÃO está instalado:** Verifica se o produto MSI especificado não está instalado. Os parâmetros são: Guid:

Sobre a Lógica de detecção: Configurações do registro usadas para a página de detecção

- **Registro:** Lista as condições de chaves do Registro usadas para determinar se a vulnerabilidade associada (ou outro tipo) existe em um dispositivo analisado. Seleciona uma chave de registro na lista para ver seus os parâmetros esperados. Se NENHUMA dessas condições forem satisfeitas, será feita a determinação de que a vulnerabilidade existe naquele dispositivo.

IMPORTANTE: Se não houver condições do Registro na lista E se não houver condições de arquivos na página Arquivos, haverá falha na análise. Em outras palavras, uma regra de detecção deve ter pelo menos uma condição de arquivo ou registro.

Se você estiver criando ou editando uma regra de detecção personalizada, clique em **Adicionar** para tornar os campos editáveis, permitindo a configuração de uma nova condição de chave do Registro e os parâmetros esperados. As regras podem incluir uma ou mais condições de registro. Para salvar uma condição do Registro, clique em **Atualizar**. Para excluir uma condição do Registro da lista, selecione-a e clique em **Remover**.

- **Chave:** Identifica a pasta e o caminho esperados da chave do Registro.
- **Nome:** Identifica o nome esperado da chave.
- **Valor:** Identifica o valor esperado da chave.
- **Exigência:** Indica se a chave do Registro deve ou não existir nos dispositivos alvo.

Sobre a Lógica de detecção: Página de Script personalizado

Use esta página se desejar gravar um script VB personalizado que verifica quaisquer outras condições nos dispositivos analisados. As propriedades do tempo de execução da varredura de segurança que podem ser acessadas com um script personalizado para reportar seus resultados são os seguintes: Detectado, Razão, Esperado e Encontrado.

Clique no botão **Usar editor** para abrir a sua ferramenta padrão de edição de scripts associada a este tipo de arquivo. Quando fechar a ferramenta você será solicitado a salvar as mudanças na página Script personalizado. Se desejar usar uma ferramenta diferente é necessário mudar a associação do tipo de arquivo.

Sobre as propriedades de vulnerabilidades personalizadas dos produtos: Página geral de informações

Use essas caixas de diálogo ao criar uma definição de vulnerabilidade personalizada que inclui um produto personalizado.

Você pode inserir um nome, fornecedor e número de versão e depois definir a lógica de detecção que determina as condições para a existência da vulnerabilidade.

Essas caixas de diálogo são similares às caixas de diálogo propriedades para as definições de vulnerabilidade publicadas. Consulte as sessões correspondentes acima.

Essa página incluí as seguintes opções:

- **Produtos afetados:** Lista de produtos afetados por esta definição de vulnerabilidade personalizada.
- **Produtos disponíveis:** Lista todos os produtos obtidos por download.
- **Filtrar produtos disponíveis por plataformas afetadas:** Restringe a lista de produtos disponíveis para somente aqueles associados à plataformas selecionadas na lógica de detecção: Página de plataformas afetadas.
- **Adicionar:** Abre a caixa de diálogo Propriedades onde é possível criar uma definição de produto personalizada.

Sobre as vulnerabilidades personalizadas dos produtos: Página Lógica de detecção

As seguintes páginas referem-se à lógica de detecção usada pela regra de detecção selecionada para determinar se a definição de vulnerabilidade (ou outro tipo de definição) existe no dispositivo analisado.

Essas caixas de diálogo são semelhantes às caixas de diálogo de lógica de detecção para download de SO conhecido e definições de vulnerabilidade de aplicativos publicadas pelos fornecedores descritos acima. Para obter mais informações sobre as opções, consulte a sessões correspondentes acima.

Sobre as vulnerabilidades personalizadas dos produtos: Lógica de detecção: Arquivos usados para a página de detecção

Consulte a Lógica de detecção: Arquivos usados para a página de detecção acima.

Sobre as vulnerabilidades personalizadas dos produtos: Lógica de detecção: Configurações das chaves de registro usadas para a página de detecção

Consulte a Lógica de detecção: Configurações do registro usadas para a página de detecção acima.

Sobre as vulnerabilidades personalizadas dos produtos: Lógica de detecção: Página de detecção de script personalizado

Consulte a Lógica de detecção: Página de Script personalizado acima.

Sobre a página Informações do patch

Use esta página para definir e configurar o arquivo de patch associado às regras (se for necessário para a correção) e a lógica usada para detectar se o patch já está instalado. Você também pode configurar comandos adicionais de instalação ou desinstalação do arquivo do patch para reparos personalizados.

Esta página e as outra sob ela referem-se ao arquivo do patch necessário para reparar uma vulnerabilidade. Estas páginas somente se aplicam se a regra de detecção selecionada permitir reparos através da distribuição de um arquivo de patch. Se a regra de detecção for limitada para análise apenas, ou se o tipo de conteúdo de segurança não usar arquivos patch para correção (como no caso de ameaças de segurança ou spyware), então essas páginas não são relevantes.

- **Reparado por patch ou somente detecção:** Clique em uma dessas opções para especificar se a regra de detecção vai somente verificar a presença da definição associada (somente detecção) ou se irá também corrigir aquela definição ao distribuir e instalar o patch necessário.
- **Informações sobre o download de patches:**
  - **URL do patch:** Exibe o caminho completo e o nome do arquivo de patch necessário para corrigir a definição selecionada, se detectada. O local de onde o arquivo de patch é descarregado.
  - **Auto-descarregável:** Indica se o download do arquivo de patch pode ser feito automaticamente do servidor de hospedagem. Você pode usar esta opção com as regras de detecção personalizadas se desejar impedir que os arquivos patch sejam descarregados através do menu de atalho da regra. Por exemplo, talvez queira impedir o descarregamento automático do patch se houver um firewall bloqueando acesso ao servidor de hospedagem.
  - **Download:** Se você estiver criando ou editando uma regra de detecção personalizada que executa correções e tiver inserido um nome de arquivo de patch e um URL, clique em **Download** para tentar fazer o download do arquivo de patch agora. Se preferir, faça o download do arquivo de correção em outro momento.
- **Informações de reparo:**
  - **Nome de arquivo único:** Identifica o nome do arquivo único executável do arquivo patch. Observe que ao fazer o download de um arquivo patch, recomenda-se que você crie um hash para o arquivo patch clicando em **Gerar Hash MD5**. (A maioria, se não todos, os arquivos patch associados à vulnerabilidades conhecidas devem ter um hash.) O arquivo de correção deve ser carregado antes da criação de um hash. Um arquivo hash é usado para garantir a integridade do arquivo de patch durante a correção (isto é, quando ele é distribuído e instalado em um dispositivo afetado). O analisador de segurança faz isso ao comparar o código hash criado quando você clica no botão Gerar hash MD5 com um novo hash gerado imediatamente antes de tentar instalar o arquivo de patch do repositório de patches. A correção continua se os dois arquivos hash coincidirem. Se eles não coincidirem (indicando que o arquivo hash foi modificado desde o download no repositório, o processo de correção é interrompido).
  - **Necessária a reinicialização:** Indica se o arquivo de patch requer uma reinicialização do dispositivo antes de concluir os seus processos de instalação e configuração no dispositivo.
  - **Instalação silenciosa:** Indica se o arquivo de patch pode concluir a sua instalação sem interação do usuário final.

Páginas Detectando o patch

As seguintes páginas referem-se à lógica de detecção usada pela regra para verificar se o patch já está instalado nos dispositivos.

IMPORTANTE: TODAS as condições especificadas para AMBAS as configurações de arquivos e do Registro devem ser atendidas para que o arquivo de patch seja detectado como já instalado em um dispositivo.

Sobre a Detecção do patch: Arquivos usados para a página de detecção de patch instalado

Esta página especifica as condições de arquivos usadas para determinar se o arquivo de patch já está instalado em um dispositivo. As opções nesta página são as mesmas que as opções na página Arquivos para a lógica de detecção da definição (veja acima). A lógica, porém, funciona de outra maneira ao detectar a instalação do patch. Em outras palavras, ao procurar uma instalação de patch, todas as condições de arquivos especificadas nesta página deverão ser atendidas para determinar uma instalação.

Sobre a Detecção do patch: Configurações do registro usadas para a página de detecção de patch instalado

Esta página especifica as condições das chaves do Registro usadas para determinar se o arquivo de patch já está instalado em um dispositivo. As opções nesta página são as mesmas que as opções na página Configurações do registro para a lógica da detecção de definições (veja acima). A lógica, porém, funciona de modo inverso neste caso. Em outras palavras, ao procurar uma instalação de patch, todas as condições do Registro especificadas nesta página devem ser atendidas para determinar uma instalação.

IMPORTANTE: TODAS as condições especificadas para AMBAS as configurações de arquivos e do Registro devem ser atendidas para que o arquivo de patch seja detectado como já instalado em um dispositivo.

Páginas de instalação e desinstalação de patch

As páginas a seguir permitirão a configuração de comandos adicionais que são executados quando o patch é instalado ou desinstalado dos dispositivos afetados.

Esta opção é disponível somente para definições personalizadas que permitem correção.

Esses comandos são úteis se você precisar programar ações específicas em dispositivos alvo para garantir a correção com êxito. Não são necessários comandos adicionais. Se não configurar nenhum comando adicional, o arquivo de correção é executado por si mesmo como padrão. Lembre-se de que se você configurar um ou mais comandos adicionais, deverá também incluir um comando que execute o arquivo de patch real com o comando Executar.

Sobre a página Comandos de instalação do patch

Use esta página para configurar comandos adicionais para uma tarefa patch de instalação. Os comandos disponíveis são os mesmos para a instalação e desinstalação patch.

- **Comandos:** Lista os comandos na ordem em que são executados nos dispositivos alvo. Seleciona um comando para ver os seus argumentos. Você pode alterar a ordem dos comandos com os botões **Mover para cima** e **Mover para baixo**. Para remover um comando da lista, selecione-o e clique em **Remover**.
- **Adicionar:** Abre uma caixa de diálogo que permite a seleção de um tipo de comando para adicionar à lista de comandos.

- **Argumentos do comando:** Exibe os argumentos que definem o comando selecionado. Os valores de um argumento podem ser editados. Para editar um argumento, clique duas vezes em seu campo **Valor** e, em seguida, digite diretamente no campo. Para todos os tipos de comandos, você também pode clicar com o botão direito do mouse no campo **Valor** para inserir uma macro/variável no argumento.

A lista seguinte contém os comandos e seus argumentos:

- **Copiar:** Copia um arquivo da origem especificada para o destino especificado no disco rígido do dispositivo alvo. Esse comando pode ser usado antes e/ou após a execução do arquivo de correção. Por exemplo, após extrair o conteúdo de um arquivo compactado com o comando Unzip, você pode desejar copiar arquivos de um local para outro.

  Os argumentos do comando Copy são: Dest (caminho completo onde deseja copiar o arquivo), sem incluir o nome do arquivo e Source (nome do caminho completo e do arquivo que deseja copiar).

- **Execute:** Executa o arquivo de patch ou qualquer outro arquivo executável nos dispositivos alvo.

  Os argumentos do comando Execute são: Path (caminho completo e nome do arquivo onde o arquivo executável reside; para o arquivo de correção, você pode usar as variáveis %SDMCACHE% e %PATCHFILENAME%), Args (opções de linha de comando para arquivo executável; note que esse campo não é requerido), Timeout (número de segundos de espera para o executável terminar antes de continuar para o próximo comando na lista, se o argumento Wait for definido como verdadeiro) e Wait (valor verdadeiro ou falso (true ou false) que determina se deve esperar para o executável terminar antes de continuar para o próximo comando na lista).

- **ButtonClick:** Clica automaticamente em um botão especificado que exibe quando um arquivo executável é executado. Você pode usar esse comando para programar um clique de botão se essa interação for requerida pelo executável.

  Para o comando ButtonClick funcionar corretamente, o argumento Wait para o comando Execute precedente deve ser definido como falso para que o executável não tenha que terminar antes de continuar para a ação de clique de botão.

  Os argumentos do comando ButtonClick são: Requerido (valor 'true' ou 'false' indicando se o botão deve ser clicado antes de continuar; se você selecionar verdadeiro (true) e o botão não puder ser clicado por qualquer razão, a correção interrompe; se você selecionar falso (false) e o botão não puder ser clicado, a correção continuará, ButtonIDorCaption (identifica o botão que você deseja que seja clicado através do respectivo texto do rótulo ou por seu ID de controle), Timeout (número de segundos que o botão que você deseja que seja clicado leva para ser mostrado quando o executável abre) e WindowCaption (identifica a janela ou caixa de diálogo onde o botão que você deseja que seja clicado está localizado).

- **ReplaceInFile:** Edita um arquivo de texto nos dispositivos alvo. Use este comando se precisar fazer modificações em um arquivo baseado em texto como, um valor específico em um arquivo .INI, antes ou depois de executar o arquivo de correção para garantir que ele executa corretamente.

  Os argumentos do comando ReplaceInFile são: Filename (caminho completo e nome do arquivo que você deseja editar), ReplaceWith (seqüência de texto exato que você deseja adicionar ao arquivo) e Original Text (seqüência de texto exato que você deseja substituir no arquivo).

- **StartService:** Inicia um serviço nos dispositivos alvo. Use este argumento para iniciar um serviço obrigatório para o arquivo de correção executar ou para reiniciar um serviço que foi requerido parar a fim do arquivo de correção para o arquivo de correção executar.

  Os argumentos do comando StartService são: Service (nome do serviço).

- **StopService:** Interrompe um serviço nos dispositivos alvo. Use este comando se um serviço precisar ser interrompido em um dispositivo antes que o arquivo de patch possa ser instalado.

  Os argumentos do comando StopService são: Service (nome do serviço).

- **Unzip:** Descompacta um arquivo nos dispositivos alvo. Por exemplo, você pode usar este comando se a correção exigir a execução ou cópia de mais de um arquivo nos dispositivos alvo.

  Os argumentos do comando Unzip são: Dest (caminho completo para onde deseja extrair o conteúdo do arquivo compactado em um disco rígido do dispositivo) e Source (caminho completo e nome de arquivo do arquivo compactado).

- **WriteRegistryValue:** Grava um valor no Registro.

  Os argumentos para o WriteRegistryValue são: Key, Type, ValueName, ValueData, WriteIfDataEmpty

Sobre a página Comandos de desinstalação do patch

Use esta página para configurar comandos adicionais para uma tarefa patch de desinstalação. Os comandos disponíveis são os mesmos para a instalação e desinstalação patch. A página de comandos patch de desinstalação, porém, inclui duas opções únicas:

- **O patch pode ser desinstalado:** Indica se o arquivo de patch pode ser desinstalado dos dispositivos corrigidos.
- **É necessário o patch original para desinstalar:** Indica se o arquivo de patch executável original precisa estar acessível no servidor núcleo para desinstalá-lo dos dispositivos analisados.

Para obter informações sobre os comandos, consulte "Sobre a página Comandos de instalação do patch" na página 634.

Sobre a caixa de diálogo Fazer o download dos patches associados

Use esta caixa de diálogo para fazer download dos arquivos executáveis de patch requeridos para corrigir a vulnerabilidade selecionada, mas que não estão disponíveis no momento no servidor núcleo (ou em outro local repositório especificado de patch). Os patches requeridos devem residir no local designado de patch a fim de o dispositivo gerenciado, que tem a vulnerabilidade detectada, ser corrigido com sucesso.

- **Nome:** Indica o nome do arquivo executável de patch.
- **Definições:** Indica a vulnerabilidade associada a este arquivo de patch.
- **Download pronto:** Indica se o download do arquivo de patch foi executado.
- **Pode fazer download:** Indica se o download do patch pode ser feito automaticamente ou se deve ser feito por um processo do Patch e Conformidade.
- **Só mostra os patches requeridos atualmente:** Exibe somente os arquivos de patch necessários para corrigir a vulnerabilidade selecionada neste momento. Em outras palavras, a lista incluirá patches que substituem os patches anteriores e não os patches anteriores em si.

- **Mostrar todos os patches associados:** Exibe uma lista abrangente de todos os patches associados para a vulnerabilidade selecionada, tenham eles sido sobrepujados ou não.
- **Download:** Clique para fazer download dos arquivos de patch do site de origem de atualização.
- **Cancelar:** Cancela a operação de download.

Ajuda de tarefas de Patch e conformidade

Sobre a caixa de diálogo Criar tarefa de análise de segurança

Use esta caixa de diálogo para criar e configurar uma tarefa agendada que executa a análise de segurança nos dispositivos alvo.

IMPORTANTE: Permissão do grupo LANDesk Script Writers é necessária
Para criar tarefas e políticas agendadas na ferramenta Patch e conformidade (para tarefas de análise de segurança e conformidade e tarefas de reparo), um usuário precisa ter permissão de grupo LANDesk Script Writers. Em outras palavras, eles precisam fazer parte de um grupo que tenha permissão de LANDesk Script Writers atribuída. Para obter mais informações sobre a administração baseada em funções, consulte "Gerenciamento de usuários" na página 38.

Você pode também executar uma análise de segurança ou de conformidade imediata por demanda em um ou mais dispositivos alvo. Clique com o botão direito no dispositivo selecionado (ou até 20 dispositivos selecionados em conjunto), clique em **Análise de segurança** e selecione configurações de análise e reparo ou clique em **Análise de conformidade**, a seguir, clique em **OK** .

Esta caixa de diálogo contém as seguintes opções:

- **Nome da tarefa:** Digite um nome exclusivo para identificar a tarefa de análise de segurança.
- **Criar uma tarefa agendada:** Adiciona a tarefa de segurança à janela Tarefas agendadas, onde você pode configurar as suas opções de agendamento e recorrência e designar dispositivos alvo.
- **Criar uma diretiva:** Adiciona a tarefa de análise de segurança à janela Tarefas agendadas, onde você pode configurar as opções da diretiva.
- **Configurações de análise e reparo:** Especifica as configurações de análise e reparo para a tarefa. As configurações de análise e reparo determinam se a varredura de segurança é mostrada em dispositivos durante a execução, as opções de reinicialização, a interação do usuário e os tipos de conteúdo de segurança analisados. Selecione configurações de análise e reparo na lista suspensa para atribuí-la à tarefa de análise de segurança que está criando. Clique em **Editar** para modificar as opções de configurações de análise e reparo selecionada. Você também pode clicar em **Configurar** para criar novas configurações de análise e reparo.

Sobre a caixa de diálogo Criação de tarefas de análise de conformidade

Use esta caixa de diálogo para criar e configurar uma tarefa que executa a análise de segurança e verifica especificamente a conformidade dos dispositivos alvo com a sua diretiva de segurança com base no conteúdo do grupo Conformidade.

NOTA: Análises de segurança e conformidade por demanda
Você também pode executar uma análise imediata de segurança ou conformidade em um ou mais dispositivos alvo. Clique com o botão direito no dispositivo selecionado (ou até 20 dispositivos

selecionados em conjunto), clique em **Análise de segurança** e selecione configurações de análise e reparo ou clique em **Análise de conformidade**, a seguir, clique em **OK** .

Esta caixa de diálogo contém as seguintes opções:

- **Nome da tarefa:** Digite um nome exclusivo para identificar a tarefa de análise de conformidade.
- **Criar uma tarefa agendada:** Adiciona a tarefa de conformidade à janela Tarefas agendadas, onde você pode configurar as suas opções de agendamento e recorrência e designar dispositivos alvo.
- **Selecionar como alvo os computadores que não tenham reportado desde:** Limita a análise de conformidade somente aos dispositivos gerenciados que não tenham reportado resultados da análise de segurança desde a data especificada.
- **Iniciar agora:** Define a tarefa de análise agendada para iniciar assim que a tarefa é adicionada à janela Tarefas agendadas. Dessa maneira, você não precisa configurar manualmente as opções de agendamento.
- **Criar uma diretiva:** Adiciona uma tarefa de análise de conformidade à janela Tarefas agendadas, onde você pode configurar as opções da diretiva.

Sobre a caixa de diálogo Mudar tarefa de configurações

Use esta caixa de diálogo para criar e configurar uma tarefa que altere as configurações padrão nos dispositivos alvo para serviços de Patch e Conformidade, incluindo:

- Configurações de análise e reparo
- Configurações de segurança da conformidade (aplica-se somente a análises de segurança da conformidade)
- Definições de substituição da variável personalizada

Com uma tarefa de alteração de configurações, você pode alterar de forma conveniente as configurações padrão do dispositivo gerenciado (gravadas no Registro local do dispositivo) sem a necessidade de redistribuir uma configuração completa de agente.

- **Nome da tarefa:** Digite um nome exclusivo para identificar a tarefa.
- **Criar uma tarefa agendada:** Conforme a tarefa à janela Tarefas agendadas, onde você pode configurar as suas opções de agendamento e recorrência, além de designar dispositivos alvo.
- **Criar uma diretiva:** Adicione a tarefa como uma diretiva à janela Tarefas agendadas onde você pode configurar as opções da diretiva.
- **Configurações de análise e reparo:** Especifica as configurações de análise e reparo para tarefas de análise de segurança. As configurações de análise e reparo determinam se a análise é mostrada em dispositivos durante a execução, as opções de reinicialização, a interação do usuário e os tipos de conteúdo de segurança analisados. Selecione uma das definições na lista suspensa. Clique em **Editar** para modificar as opções das definições selecionadas. Clique em **Configurar** para criar novas definições. Para obter mais informações, consulte a caixa de diálogo "Sobre as páginas da caixa de diálogo Definições de análise e reparo (e conformidade)" na página 643.
- **Definições de conformidade:** Especifica as configurações de conformidade usadas para as tarefas de análise conformidade. As Definições de conformidade determinam quando e como ocorre uma análise de conformidade, se a correção é automática, e/ou qual ação tomar quando o LANDesk Antivirus detecta uma infecção de vírus nos dispositivos alvo.

- **Configurações de variáveis personalizadas a serem substituídas:** Especifica as definições de sobrescrição das variáveis personalizadas em dispositivos quando são analisados por definições de segurança que incluem variáveis personalizadas (como, por exemplo, ameaças de segurança e vírus). As configurações de substituição de variáveis personalizadas permitem especificar os valores que você deseja ignorar durante uma análise de segurança. Isso é muito útil em situações em que você não deseja que um dispositivo analisado seja identificado como vulnerável de acordo com as configurações de variáveis personalizadas padrão de uma definição. Selecione uma das definições na lista suspensa. Na lista suspensa, você também pode selecionar a remoção das configurações de substituição de variáveis personalizadas dos dispositivos alvo. A opção **Remover definições das variáveis personalizadas** permite limpar um dispositivo para que as definições de variável personalizada funcionem completamente. Clique em **Editar** para modificar as opções das definições selecionadas. Clique em **Configurar** para criar novas definições. Para obter mais informações, consulte "Sobre a caixa de diálogo Configurar as definições da variável personalizada a ser substituída" na página 650.

Sobre a caixa de diálogo Criar tarefa de reinicialização

Use esta caixa de diálogo para criar e configurar uma tarefa genérica de reinício.

Uma tarefa de reinicialização pode ser útil quando você desejar instalar patches (sem reinicializar) como um processo único e, em seguida, reinicializar os dispositivos corrigidos como outra tarefa separada. Por exemplo, você pode executar uma análise ou uma instalação de patch durante o dia, e depois distribuir uma tarefa de apenas reinício quando for mais conveniente para os usuários finais.

- **Nome da tarefa:** Identifica a tarefa com um nome exclusivo.
- **Criar uma tarefa agendada:** Cria uma tarefa de reinicialização na janela Tarefas agendadas quando você clica em **OK**.
- **Criar uma diretiva:** Cria uma diretiva de reinicialização quando você clica em **OK**.
- **Configurações de análise e reparo:** Especifica quais configurações de inicialização das configurações de de análise e reparo são usadas para a tarefa, visando determinar os requisitos de reinicialização e a ação nos dispositivos alvo. Selecione configurações de análise e reparo na lista suspensa ou clique em **Configurar** para criar novas configurações de análise e reparo.

Sobre a caixa de diálogo Criar tarefa de reparo

Use esta caixa de diálogo para criar e configurar uma tarefa de reparo (remediação) para os tipos de definição a seguir: vulnerabilidades, spyware, atualizações de software da LANDesk, definições personalizadas e ameaças de segurança com um patch associado. A opção de reparo agendado não é aplicável aos aplicativos bloqueados.

Essa caixa de diálogo contém as seguintes páginas:

- "Sobre Criar tarefa de reparo: Página geral" na página 639
- "Sobre Criar tarefa de reparo: Página Patches" na página 640

Sobre Criar tarefa de reparo: Página geral

- **Nome da tarefa:** Identifica a tarefa de reparo com um nome exclusivo. O padrão é o nome da definição selecionada ou do grupo personalizado. Se preferir, você pode editar esse nome.
- **Reparo como uma tarefa agendada:** Cria uma tarefa de reparo de segurança na janela Tarefas agendadas quando você clica em **OK**.

- **Dividir em tarefas por etapas e tarefas de reparo:** (Opcional) Permite criar duas tarefas separadas na ferramenta de Tarefas agendadas; uma para estágio dos arquivos requeridos no cache local do dispositivo alvo e outra para a própria instalação dos arquivos de patch nos dispositivos afetados.
    - **Selecionar os computadores a serem reparados:** Especifica quais dispositivos devem ser adicionados à tarefa de reparo agendada. Você pode escolher nenhum dispositivo, todos os dispositivos afetados (dispositivos onde a definição foi detectada pela última análise de segurança) ou somente os dispositivos afetados que também foram selecionados (esta última opção estará disponível somente se você acessar a caixa de diálogo Agendar reparo a partir de uma caixa de diálogo de informações de Segurança e patch).
    - **Usar multidifusão:** Habilita a Multidifusão dirigida para a distribuição de patches para dispositivos. Clique nesta opção e em **Opções de multidifusão** se desejar configurá-las. Para obter mais informações, consulte "Sobre a caixa de diálogo Opções de multidifusão" na página 640.
- **Reparo como uma diretiva:** Cria uma diretiva de reparo de segurança quando você clica em **OK**.
    - **Adicionar consulta representando dispositivos afetados:** Cria uma nova consulta com base na definição selecionada e a aplica à diretiva. Esta diretiva baseada em pesquisa irá procurar dispositivos afetados pela definição selecionada e distribui o patch associado.
    - **Fazer download do patch somente dos parceiros locais:** Restringe a distribuição de patches de modo que ela ocorrerá somente se o arquivo de patch estiver localizado no cache local do dispositivo ou na mesma sub-rede. Essa opção preserva a largura de banda da rede, mas observe que para a instalação do patch ser bem-sucedida, o arquivo de patch deve estar em um desses dois locais.
    - **Fazer download somente do patch (Não reparar):** Faz download do arquivo de patch no repositório patches, mas não distribui o patch. Você pode usar essa opção se desejar recuperar o arquivo de patch em uma etapa intermediária para teste antes da distribuição real.
- **Configurações de análise e reparo:** Especifica que configurações de análise e reparo é usada para a tarefa de reparo de forma a determinar se a análise de segurança é exibida nos dispositivos quando é executada. Selecione as configurações de análise e reparo na lista suspensa ou clique em **Configurar** para criar novas configurações de análise e reparo.

Sobre Criar tarefa de reparo: Página Patches

Use esta página para mostrar apenas os patches requeridos ou todos os patches associados para a vulnerabilidade selecionada. (**NOTA:** Os campos nesta página são os mesmos que campos em "Sobre a caixa de diálogo Fazer o download dos patches associados" na página 636.)

Você também pode fazer o download de patches diretamente desta página se eles já não tiverem sido inseridos no repositório de patches (clique em **Download**).

Sobre a caixa de diálogo Opções de multidifusão

Use essa caixa de diálogo para configurar as seguintes opções de Multidifusão dirigida para tarefa agendada de reparo de segurança:

- **Descobrimento de domínio de multidifusão:**
    - **Usar o Descobrimento de domínio de multidifusão:** Selecione esta opção se desejar que a Multidifusão dirigida descubra um domínio para este trabalho. Essa opção não salvará os resultados do descobrimento de domínio para que sejam reutilizados.

    - **Usar descobrimento de domínio de multidifusão e salvar resultados:** Selecione esta opção apenas se desejar que a Multidifusão dirigida descubra um domínio para este trabalho e salve os resultados para uso posterior, economizando tempo em multidifusões subseqüentes.
    - **Usar os resultados do último descobrimento de domínio de multidifusão:** Use esta opção quando a Multidifusão dirigida descobrir um domínio cujos resultados foram salvos.
- **Fazer com que o representante de domínio ative os computadores:** Use esta opção se desejar que os computadores que ofereçam suporte à tecnologia Wake On LAN sejam ligados para que possam receber a multidifusão.
- **Número de segundos a esperar após Wake On LAN:** Tempo de espera dos representantes de domínio para fazer a multidifusão depois que o pacote Wake On LAN for enviado. O período de espera padrão é de 120 segundos. Se alguns computadores na rede demorarem mais do que 120 segundos para a reinicialização, você deverá aumentar esse valor. O valor máximo permitido é 3600 segundos (uma hora).

As opções abaixo permitem configurar parâmetros de Multidifusão dirigida específicos para tarefas. Os padrões devem ser utilizados na maioria das multidifusões. A seguir está descrição das opções:

- **Número máximo de representantes do domínio de multidifusão trabalhando simultaneamente:** Não mais do que este número de representantes executará uma multidifusão simultaneamente.
- **Limitar o processamento dos computadores nos quais a multidifusão falhou:** Quando um dispositivo apresentar falha ao receber o arquivo através de multidifusão, ele fará o download do arquivo do servidor Web ou de arquivos. Esse parâmetro pode ser usado para limitar o número de dispositivos que obterão o arquivo de uma só vez. Por exemplo, se o número máximo de segmentos fosse 200 e o número máximo de segmentos de falha de multidifusão fosse 20, a caixa de diálogo Tarefa personalizada processaria, por vez, não mais do que 20 computadores que apresentassem falha de multidifusão. A caixa de diálogo Tarefa personalizada processará no máximo 200 dispositivos por vez se eles receberem o multidifusão com sucesso, mas não mais do que 20 desses 200 segmentos processarão os dispositivos que apresentarem falha na tarefa de multidifusão. Se esse valor for definido como 0, a caixa de diálogo Tarefa personalizada não executará a parte de distribuição da tarefa para nenhum computador que tiver apresentado falha na multidifusão.
- **Número de dias que os arquivos ficam no cache:** Tempo em que o arquivo sendo transmitido por multidifusão pode permanecer no cache de cada computador alvo. Após esse período, o arquivo será automaticamente removido.
- **Número de dias que os arquivos ficam no cache do representante de domínio de multidifusão:** Tempo em que o arquivo sendo transmitido por multidifusão pode permanecer no cache do representante de domínio de multidifusão. Após esse período, o arquivo será automaticamente removido.
- **Número mínimo de milissegundos entre as transmissões de pacotes (WAN ou Local):** Tempo mínimo de espera entre envios de pacotes de multidifusão.

Esse valor somente será usado quando o representante de domínio não estiver fazendo a multidifusão de um arquivo a partir de seu próprio cache. Se esse parâmetro não for especificado, o tempo de inatividade mínimo padrão armazenado no computador do representante da sub-rede/domínio será usado. É possível usar esse parâmetro para limitar o uso de largura de banda na WAN.

- **Número máximo de milissegundos entre as transmissões do pacote (WAN ou Local):** Tempo máximo de espera entre envios de pacotes de multidifusão. Para obter mais informações, consulte Número mínimo de milissegundos entre as transmissões do pacote acima.

Sobre a caixa de diálogo Desinstalar o patch

Use esta caixa de diálogo para criar e configurar uma tarefa de desinstalação para patches que foram distribuídos nos dispositivos afetados.

- **Nome da tarefa:** Identifica a tarefa com um nome exclusivo. O padrão é o nome do patch. Se preferir, você pode editar esse nome.
- **Revista como uma tarefa agendada:** Cria uma tarefa de desinstalação do patch na janela Tarefas agendadas quando você clica em **OK**.
    - **Selecionar alvos:** Especifica quais dispositivos devem ser adicionados à tarefa de desinstalação de patches. Você pode escolher nenhum dispositivo, todos os dispositivos com o patch instalado ou somente os dispositivos com o patch instalado que também estão selecionados (esta última opção está disponível somente quando você acessar a caixa de diálogo Revista patch de dentro de uma caixa de diálogo de dispositivo Informações de segurança e patch).
- **Se o patch original for necessário:**
    - **Usar multidifusão:** Habilita a Multidifusão dirigida para distribuição da tarefa de desinstalação de patches para os dispositivos. Clique nesta opção e em **Opções de multidifusão** se desejar configurá-las. Para obter mais informações, consulte "Sobre a caixa de diálogo Opções de multidifusão" na página 640.
- **Remoção como uma diretiva:** Cria uma diretiva de desinstalação de patch na janela Tarefas agendadas quando você clica em **OK**.
    - **Adicionar consulta representando dispositivos afetados:** Cria uma nova consulta com base no patch selecionado e a aplica à diretiva. Esta diretiva baseada em pesquisa busca os dispositivos com o caminho selecionado instalado, e o desinstala.
- **Configurações de análise e reparo:** Especifica que configurações de análise e reparo é usada para a tarefa de desinstalação de forma a determinar se a análise de segurança é exibida nos dispositivos, as opções de reinicialização, as informações sobre o local do MSI, etc. Selecione as configurações de análise e reparo na lista suspensa ou clique em **Configurar** para criar novas configurações de análise e reparo.

Sobre a caixa de diálogo Coletar informações de histórico

Use esta caixa de diálogo para compilar dados sobre as vulnerabilidades analisadas e detectadas nos dispositivos gerenciados. Estas informações são usadas para os relatórios de segurança. Você pode obter os dados imediatamente ou criar uma tarefa para coletar dados por um período de tempo especificado.

Esta caixa de diálogo contém as seguintes opções:

- **Nome da tarefa:** Identifica a tarefa de obtenção de informações de histórico com um nome exclusivo.
- **Manter dados de histórico por:** Especifica o tempo (em dias) durante o qual os dados serão coletados. É possível especificar de 1 a 3.000 dias.
- **Compilar dados de relatório para definições publicadas menos que:** Restringe o relatório aos dados sobre vulnerabilidades publicados dentro do período especificado.
- **Aviso:** Mostra uma mensagem no console do servidor núcleo se uma tarefa de coleta de histórico não for executada no período especificado.
- **Coletar agora:** Coleta imediatamente os dados atuais para vulnerabilidades analisadas e não analisadas detectadas.

- **Criar tarefa:** Adiciona a tarefa à janela Tarefas agendada, onde você pode configurar as suas opções de agendamento e recorrência, além de designar dispositivos alvo.
- **Limpar:** Remove completamente os dados sobre vulnerabilidades coletadas até este ponto.

Ajuda da configurações de Patch e conformidade

Sobre a caixa de diálogo Definições da configuração de análise e reparo (e conformidade)

Use esta caixa de diálogo para gerenciar as configurações de análise e reparo (e conformidade). Quando definidas, você pode aplicar as configurações a tarefas de análise de segurança, tarefas de análise de conformidade, tarefas de reparo, tarefas de desinstalação e tarefas de reinicialização.

Esta caixa de diálogo contém as seguintes opções:

- **Novo:** Abra a caixa de diálogo de configurações onde você possa configurar as opções pertinentes a tipos de configurações específicas.
- **Editar:** Abre a caixa de diálogo de definições onde você pode modificar as configurações selecionadas.
- **Copiar:** Abre uma cópia das configurações selecionadas como um modelo que pode ser modificado e renomeado.
- **Excluir:** remove as configurações selecionadas do banco de dados.

  NOTA: As configurações selecionadas podem estar associadas no momento com uma ou mais tarefas ou dispositivos gerenciados. Se você decidir excluir a configuração: dispositivos com aquelas definições ainda a reterão e continuarão a usá-las até que uma nova tarefa de mudança de configurações seja distribuída; as tarefas agendadas com aquelas configurações ainda serão executadas nos dispositivos alvo, assim como as tarefas do agendador local com aquelas configurações até que uma nova configuração seja distribuída.

- **Fechar:** Fecha a caixa de diálogo sem aplicar nenhuma configuração à tarefa.

Sobre as páginas da caixa de diálogo Definições de análise e reparo (e conformidade)

Use esta caixa de diálogo para criar e editar uma configuração de análise e reparo. As configurações de análise e reparo determinam se a varredura de segurança é mostrada em dispositivos durante a execução, as opções de reinicialização, a interação do usuário e os tipos de conteúdo analisados.

NOTA: Observação sobre as configurações de conformidade
As informações nesta caixa de diálogo também podem ser aplicadas às análises de conformidade, com a guia **Conformidade** substituindo a página **Análise**. Consulte a seção Sobre a página Conformidade abaixo para obter detalhes sobre as configurações específicas que se aplicam às análises de conformidade.

NOTA: Observação sobre as configurações da tarefa de reinicialização
As configurações da página **Reinicializar** desta caixa de diálogo também podem ser usadas para uma

tarefa de reinicialização somente.

Você pode criar quantas configurações de análise e reparo desejar e editá-las a qualquer momento. Por exemplo, você pode definir configurações de análise e reparo com uma situação específica de notificação e reinicialização para dispositivos de desktop e outras configurações de análise e reparo com diferentes opções de reinicialização para servidores. Ou, pode definir configurações de análise de reparo para a análise de vulnerabilidade Windows e outra para análise de spyware, etc.

Quando definidas, você pode aplicar as configurações de análise e reparo às tarefas de análise de segurança, tarefas de reparo, tarefas de desinstalação e tarefas de reinicialização.

Configurações de análise e reparo

- **Nome:** Identifica as configurações com um nome exclusivo. Esse nome é exibido na lista suspensa de configurações em uma caixa de diálogo da tarefa de segurança.

A caixa de diálogo configurações contém as seguintes páginas:

- "Sobre a página Configurações gerais" na página 644
- "Sobre a página Opções de análise" na página 645
- "Sobre a página Configurações de conformidade" na página 645
- "Sobre a página Opções de reparo" na página 646
- "Sobre a página Informações de MSI" na página 647
- "Sobre a página Opções de reinicialização" na página 647
- "Sobre a página Configurações de rede" na página 648
- "Sobre a página Configuração piloto" na página 648
- "Sobre a página Análise de spyware" na página 648

Sobre a página Configurações gerais

- **Exibir a caixa de diálogo andamento:** Habilita a varredura de segurança para mostrar informações sobre os dispositivos do usuário final enquanto estiver sendo executada. Selecione uma opção da lista suspensa (Nunca, Sempre, Somente quando em reparo) para determinar se e quando você deseja mostrar a atividade do analisador e se deseja configurar outras opções de tela e interação neste diálogo. Se selecionar Nunca, nenhuma das outras opções desta página estará disponível para configurar e a análise será executada de modo transparente nos dispositivos. Se selecionar Sempre, você pode configurar as outras opções.
- **Ocultar se o usuário estiver mostrando uma apresentação:** Não mostra o analisador de segurança nos dispositivos de usuário final se a aplicação do Microsoft Office PowerPoint estiver sendo executada no dispositivo.
- **Permitir ao usuário cancelar:** Mostra um botão Cancelar no diálogo da varredura de seguraná no dispositivo do usuário final. Clique nesta opção se você desejar que o usuário final possa cancelar a operação de análise. Se esta opção não for selecionada, a caixa de diálogo não exibirá o botão Cancelar e o usuário final não poderá interromper a análise.
- **Quando a reinício não for necessária:**
  - **Solicitar intervenção do usuário final antes de fechar:** Para uma análise ou tarefa de reparo que não necessite de reinicialização para concluir sua operação completa, clique nesta opção se desejar que a análise avise ao usuário final antes que a sua caixa de diálogo de exibição seja fechada no dispositivo. Se você selecionar esta opção e o usuário final não responder, a caixa

de diálogo permanecerá aberta o que pode fazer com que outras tarefas agendadas expirem o tempo limite.

- **Fechar após o limite:** Para uma tarefa de análise ou reparo que não necessite de reinicialização, clique nesta opção se desejar que a caixa de diálogo de exibição do analisador feche após a duração especificada.

- **Uso da CPU durante a análise:** Permite ajustar detalhadamente o uso da CPU pelo analisador de segurança a fim de melhorar o desempenho geral do sistema. Se houver vários processos em execução e maximização da utilização da CPU nos dispositivos simultaneamente, você pode reduzir esta configuração para o analisador de segurança.
- **Status da tarefa agendada:** Indica o nível de informações enviadas para a ferramenta de Tarefas agendadas sobre a tarefa de análise de segurança agendada.

Sobre a página Opções de análise

- **Analisar para:** Especifica quais tipos de conteúdo você deseja analisar com esta tarefa. Você pode selecionar um grupo personalizado (pré-configurado) ou tipos específicos de conteúdo. Você só pode selecionar os tipos de conteúdo para os quais tiver assinatura de conteúdo do LANDesk Security Suite. Além disso, as definições de segurança reais que são analisadas dependem do conteúdo do grupo Analisar na janela do Patch e Conformidade. Em outras palavras, se você selecionar vulnerabilidades e ameaças de segurança nesta caixa de diálogo, somente as vulnerabilidades e ameaças de segurança residindo atualmente nos respectivos grupos Analisar serão analisadas.
- **Repara imediatamente todos os itens detectados:** Indica que qualquer risco de segurança identificado por este grupo em particular será corrigido automaticamente.
- **Habilitar autofix:** Indica que a análise de segurança irá distribuir e instalar automaticamente os arquivos patch associados necessários para quaisquer definições de vulnerabilidade ou personalizadas que detectar nos dispositivos analisados. Esta opção se aplica somente às tarefas de análise de segurança. Para que a correção automática funcione, o arquivo de patch também deve possuir a correção automática habilitada.

Sobre a página Configurações de conformidade

NOTA: Análises de segurança de conformidade
Lembre-se de que as opções na página Conformidade se aplicam apenas às análises de segurança de conformidade.

- **Analisando:**
  - **Análise freqüente do grupo Conformidade:** Executa freqüentemente uma análise de segurança com base no conteúdo do grupo Conformidade. A análise básica de segurança frequente é definida na configuração inicial de agente, mas é possível substituí-la com as opções nessa página. Só é possível especificar a execução da análise de segurança de conformidade quando um usuário estiver conectado ao dispositivo gerenciado.
  - **Análise após a mudança no endereço IP:** Faz uma análise de segurança de conformidade sempre que o endereço IP for modificado nos dispositivos gerenciados. Por exemplo, se um laptop for reconectado à sua rede e receber um endereço IP diferente do anterior.
  - **Desabilitação da análise freqüente de segurança na configuração do Agente:** Indica que a definição da análise freqüente de segurança através da configuração do agente dispositivo será desligada, e que as definições de análise freqüente aqui definidas serão usadas para uma análise de segurança de conformidade.

- **Ações:**
  - **Habilitar autofix:** Indica que a análise de segurança irá distribuir e instalar automaticamente os arquivos patch associados necessários para quaisquer definições de vulnerabilidade que detectar nos dispositivos analisados. Esta opção se aplica somente às tarefas de análise de segurança e conformidade. Para que a correção automática funcione, ela deve estar ativada.
  - **Repara imediatamente todos os itens detectados:** Todas as vulnerabilidades detectadas são corrigidas, mesmo se o autofix não estiver habilitado nos patches associados.
  - **Reforçar a análise de 802.1X suportado:** Garante que os dispositivos ativados 802.1X anallisados em busca de conformidade de segurança usando estas configurações sejam tanto acessados quando colocados em quarentena com base em estarem ou não em conformidade com as suas diretivas de segurança personalizadas.
- **Se um vírus não puder ser removido ou entrar em quarentena (somente LANDesk Antivirus):** As duas opções a seguir se aplicam somente ao LANDesk Antivirus e fornecem um método de disparo da análise antivírus ou iniciam uma análise de segurança completa que verifica os dispositivos alvo configurados com estas definições para conformidade com a sua diretiva atual de segurança. Em outras palavras, se o dispositivo estiver saudável ou não saudável. Voce pode selecionar uma ou ambas as opções. A ação descrita por essas opções ocorre sempre que um vírus é detectado no dispositivo e não pode ser removida ou entrar em quarentena. (**NOTA:** Como pré-requisito para realizar esse tipo de análise, é necessário primeiro adicionar a configuração de antivírus pré-definida AV-110 ao grupo Conformidade. Também é necessário adicionar quaisquer outras configurações que deseje usar para definir a diretiva de segurança para o grupo de conformidade.)
  - **Analisar dispositivos imediatamente para verificar a conformidade:** Se for detectado vírus o qual não pode ser removido ou colocado em quarentena, é iniciada, imediatamente, uma análise de segurança de conformidade (pelo analisador de segurança, não o analisador de antivírus).
  - **Executar verificação de controle de acesso à rede se o dispositivo não estiver em funcionamento:** Se um vírus for detectado e não puder ser removido ou colocado em quarentena, é iniciada, imediatamente, uma verificação de controle de acesso à rede (pelo LANDesk NAC).

Sobre a página Opções de reparo

- **Antes de reparar, instalar ou desinstalar um patch:** Selecione se deseja que o reparo comece imediatamente ou se quer que apareça um prompt no dispositivo do usuário com a mensagem e os controles de interação como configurados com as opções abaixo ou se quer aguardar para executar o reparo até que o dispositivo seja bloqueado ou o usuário tenha feito o logoff.
- **Mensagem:** Digite uma mensagem no diálogo do analisador de segurança no dispositivo do usuário final QUANDO a tarefa de análise de segurança detectar qualquer uma das definições especificadas no dispositivo analisado. Você pode personalizada esta mensagem, dependendo do tipo de análise de segurança que estiver executando.
- **Se não houver resposta do usuário final:**
  - **Aguardar resposta do usuário antes de reparar, instalar ou remover:** Clique nesta opção se desejar que o analisador continue aguardando indefinidamente em um prompt de operação de arquivo de patch que não receba resposta.
  - **Depois do limite, automaticamente:** Clique nesta opção se desejar que o analisador continue e execute a operação de arquivo de patch automaticamente ou feche sem executar a operação, após a duração especificada, em um prompt de operação de arquivo de patch que não receba resposta.

- **Iniciar reparo mesmo se:**
  - **O usuário está executando uma apresentação:** Indica que a correção iniciará independentemente de a aplicação do Microsoft Office PowerPoint estar em execução no dispositivo.
  - **Reinicialização já pendente:** Indica que a correção começará sem aguardar a operação de reinicialização.
- **Largura de banda máxima quando descarregar da fonte:** Especifica a porcentagem de largura de banda que desejar usar para o download do arquivo de patch do repositório de patches para dispositivos analisados. Você pode usar estas configurações para equilibrar o tráfego da rede para grandes distribuições de arquivo de patch.
- **Largura de banda máxima quando descarregar de parceiro:** Especifica a porcentagem de largura de banda que desejar usar para o download do arquivo de patch do computador parceiro. Você pode usar estas configurações para equilibrar o tráfego da rede para grandes distribuições de arquivo de patch.

Sobre a página Informações de MSI

Use esta página se um arquivo de patch precisar acessar o recurso de instalação do produto originador para instalar arquivos suplementares necessários. Por exemplo, talvez precise fornecer esta informação quando estiver tentando aplicar um patch para o Microsoft Office ou outro suite de produtos.

- **Local do pacote original:** Insira o caminho UNC para a imagem do produto.
- **Credentiais para usar quando fizer referência ao local original do pacote:** Insira um nome de usuário e senha válidos para autenticar o compartilhamento de rede acima especificado.
- **Ignorar a opção de linha de comando /overwriteoem:** Indica que o comando para substituir as instruções específicas de OEM será ignorado. Em outras palavras, as instruções de OEM são executadas.
- **Executar como informação: Credenciais para a execução de patches:** Insere um nome de usuário e senha válidos para identificar o usuário conectado para execução de patches.

Sobre a página Opções de reinicialização

- **Ao decidir se irá reinicializar:** Especifique a forma como deseja que o analisador de segurança funcione quando uma análise ou tarefa de reparo tentar reinicializar um dispositivo, por qualquer motivo. Você pode escolher que o dispositivo nunca reinicialize, reinicialize somente se necessário ou sempre reinicialize.
- **Ao reinicializar:**
  - **Avisar o usuário antes de reinicializar:** Clique nesta opção se desejar que o analisador de segurança avise ao usuário quando ocorrer uma reinicialização. Se selecionou esta opção, poderá configurar as opções de reinício acompanhantes, a seguir.
  - **Se não houver ninguém conectado, reinicializar imediatamente sem aviso ou demora:** Garante que a reinicialização ocorrerá automaticamente no caso de ninguém estar conectado no dispositivo no momento.
  - **Permitir ao usuário pospor o reinício:** Mostra um botão de adiamento no prompt de reinicialização do dispositivo do usuário final. Especificar o intervalo e o número de vezes que o usuário final pode pospor a reinício. O intervalo (ou adiamento) inicia com o próximo poll do agendador local. (Note que devido à operação do agendador local o tempo de atraso mínimo é de 10 minutos.)

- **Permitir ao usuário reinicializar:** Mostra um botão de cancelamento no prompt de reinicialização do dispositivo do usuário final.
- **Mensagem de reinicialização:** Digite uma mensagem na caixa de diálogo do analisador de segurança no dispositivo do usuário final QUANDO a tarefa de análise de segurança solicitar a confirmação do usuário final antes de tentar reinicializar o dispositivo.
- **Aguardar resposta do usuário antes de reinicializar:** Clique nesta opção se desejar que o analisador continue aguardando indefinidamente em um prompt de reinicialização que não receba resposta. Se não houver resposta, o aviso continuará aberto.
- **Depois do limite, automaticamente:** Clique nesta opção se desejar que o analisador prossiga automaticamente e reinicialize, atrase ou feche o prompt sem reinicialização, após a duração especificada, em um prompt de reinicialização que não receba resposta.

Sobre a página Configurações de rede

Use esta página para identificar um servidor núcleo alternativo que pode ser usado para análise e correção de segurança se o servidor núcleo principal não estiver disponível.

- **Comunicação com o servidor núcleo alternativo:** Habilita a comunicação com um servidor alternativo.
- **Nome do servidor:** Digite o nome de um servidor núcleo LANDesk válido e licenciado.

IMPORTANTE: A sintaxe do campo nome do servidor deve ser: <nome do servidor>:<número da porta> onde o número da porta é a porta protegida 443 para transmissão SSL. Se digitar apenas um nome de servidor sem especificar a porta 443, a porta padrão 80 é definida automaticamente, a qual é a porta HTTP padrão.

Sobre a página Configuração piloto

Use esta página para criar e configurar um grupo piloto para testar as definições de segurança antes de executar uma distribuição mais ampla na rede inteira.

- **Analisar e reparar periodicamente as definições nos seguintes grupos:** Ativar os recursos de análise de seguraça piloto. Uma vez marcada esta opção, é necessário selecionar um grupo personalizado a partir da lista suspensa.
- **Mudar configurações:** Abra a caixa de diálogo Planejamento onde você poderá definir os parâmetros para a análise de segurança. Clique no botão **Ajuda** para ver os detalhes

Sobre a caixa de diálogo Reparo e análise piloto agendada periodicamente

Esta caixa de diálogo é compartilhada por várias tarefas de gerenciamento LANDesk. Para obter detalhes sobre as opções nessa caixa de diálogo, consulte "Sobre a caixa de diálogo Agenda" na página 237.

Sobre a página Análise de spyware

Use esta página para substituir (ou cancelar) as configurações de spyware de uma configuração de agente do dispositivo.

A detecção de spyware em tempo real monitora dispositivos para verificar processos iniciados recentemente que tentam modificar o registro local. Se o spyware for detectado, a análise de segurança no dispositivo avisa o usuário final para removê-lo.

Essa página contém as seguintes opções:

- **Substituir definições da configuração do cliente:** Substitui definições de spyware existentes em dispositivo configurados inicialmente através de uma configuração de agente. Use as opções abaixo para especificar as novas definições de spyware que deseja distribuir para os dispositivos alvo.
- **Configurações:**
  - **Permite bloqueamento de spyware em tempo real:** Ativa a monitoração e o bloqueamento de spyware em tempo real nos dispositivos com essa configuração de agente.

    NOTA: Para a análise e detecção de spyware em tempo real funcionar, é necessário habilitar manualmente o recurso de correção automática (autofix) para qualquer definição de spyware descarregada que quiser incluir em uma análise de segurança. As definições de spyware obtidas por download não vêm com o autofix habilitado como padrão.

  - **Notificar o usuário quando o spyware for bloqueado:** Exibe uma mensagem que informa o usuário final sobre a detecção e correção de um programa spyware.
  - **Se um aplicativo não for reconhecido como spyware, peça aprovação ao usuário antes de ser instalado:** Mesmo se o processo detectado não for reconhecido como spyware de acordo com a lista atual de definições de spyware do dispositivo, o usuário final será avisado antes que o software seja instalado no computador.

Sobre a caixa de diálogo Configurar as definições da variável personalizada a ser substituída

Use esta caixa de diálogo para gerenciar as configurações de substituições de variáveis personalizadas. Quando configuradas, você aplica as configurações de substituição de variáveis personalizadas a uma tarefa de configurações de alteração e a distribui aos dispositivos alvo para alterar (ou remover) as configurações de substituição de variáveis personalizadas padrão.

As substituições de variáveis personalizadas permitem configurar exceções para os valores de variáveis personalizadas. Em outras palavras, com essas definições você pode ignorar uma condição variável personalizada específica para que um dispositivo analisado não apareça como vulnerável.

Esta caixa de diálogo contém as seguintes opções:

- **Novo:** Abre a caixa de diálogo Configurar as definições da variável personalizada a ser substituída onde você pode definir as opções.
- **Editar:** Abre a caixa de diálogo de configurações onde você pode modificar as configurações de substituição de variáveis personalizadas.
- **Copiar:** Abre uma cópia das configurações selecionadas como um modelo que pode ser modificado e renomeado.
- **Excluir:** remove as configurações selecionadas do banco de dados.

  NOTA: As configurações selecionadas podem estar associadas no momento com uma ou mais tarefas ou dispositivos gerenciados. Se você decidir excluir as configurações, os dispositivos com aquelas definições ainda a reterão e continuarão a usá-las até que uma nova tarefa de mudança de configurações seja distribuída; as tarefas agendadas com aquelas configurações ainda serão executadas nos dispositivos alvo, assim como as tarefas do agendador local com aquelas configurações até que uma nova configuração seja distribuída.

- **Fechar:** Fecha a caixa de diálogo sem aplicar nenhuma configuração à tarefa.

Sobre a caixa de diálogo Configurar as definições da variável personalizada a ser substituída

Use esta caixa de diálogo para criar exceções de definições das variáveis personalizadas. Algumas definições de ameaça de segurança de configuração de sistema têm parâmetros que foram mudados antes de incluí-las na análise de segurança. Normalmente, as definições de antivírus têm também configurações variáveis personalizadas.

Com as variáveis personalizadas é possível ajustar a análise de ameaça de segurança modificando um ou mais valores para que o analisador verifique as condições definidas e determine um dispositivo para ser vulnerável somente se aquela condição for satisfeita (por exemplo, o valor especificado é detectado). As variáveis personalizadas são configurações globais, de modo que quando analisar uma definição de segurança incluindo uma variável personalizada, ela será sempre identificada como vulnerável se a condição da variável personalizada for satisfeita.

IMPORTANTE: Direito Editar variáveis personalizadas necessário
Para editar as configurações de variáveis personalizadas e configurar as opções de substituição de variáveis personalizadas, o usuário LANDesk deve possuir o direito de administração com base na função Editar variáveis personalizadas. Os direitos são configurados com a ferramenta **Usuários**.

As informações das configurações de substituição de variáveis personalizadas são exibidas no Inventário do dispositivo.

Sobre a caixa de diálogo Configurações de grupo de definições

Use esta caixa de diálogo para criar, editar e selecionar configurações que controlam como e onde as definições de segurança foram obtidas por download com base em seu tipo e/ou severidade.

Esta caixa de diálogo contém as seguintes opções:

- **Tipo de definições e filtros de severidade:** Lista as configurações do grupo de definições.
- **Tipo:** Mostra o tipo de definição para as configurações do grupo selecionado.
- **Gravidade:** Mostra a severidade de definição para as configurações do grupo selecionado.
- **Comparação:**
- **Status:** Mostra o status (Não analisar, Analisar e Não atribuído) para as definições compatíveis às configurações de grupo quando as mesmas são obtidas por download. O status corresponde aos nós de grupo na visualização em árvore do Patch e Conformidade. Não atribuído, é o status padrão.
- **Grupo(s):** Mostra o grupo ou os grupos onde as definições de segurança compatíveis com o tipo e o critério de severidade especificado acima são colocadas. Você pode adicionar e excluir quantos grupos personalizados você quiser.
- **Correção automática:** Se você especificou que as definições de segurança obtidas por download foram definidas para o status Análise (colocada no grupo Análise), selecione esta opção se deseja que as vulnerabilidades tenham a auto-correção ativada.
- **Desabilitar substituído:**

Sobre a caixa de diálogo Propriedades da definição de filtros

Use esta caixa de diálogo para definir as configurações do grupo de definições Essas configurações controlam como e onde as definições de segurança são obtidas por download com base no seu tipo e/ou severidade.

Esta caixa de diálogo contém as seguintes opções:

- **Filtro:** Define qual conteúdo de segurança (definições) serão colocadas no grupo ou grupos selecionados abaixo.
    - **Tipo de definição:** Seleciona o tipo de definição desejado para download com o status e localização desejados.
    - **Gravidade:** Seleciona a gravidade para o tipo de definição especificada. Se o tipo for compatível mas a severidade não, a definição não será filtrada por estas configurações.
- **Ação:** Define o que você deseja com as definições de download e onde você deseja colocá-las.
    - **Definir status:** Seleciona o status para as definições obtidas por download. As opções são: Não analisar, Analisar e Não atribuído.
    - **Definir auto correção:** Selecione a auto-correção se o status for Análise e você desejar correr o risco de seguraça de ser corrigod automaticamente assim que for detectado.
    - **Colocar definição em grupos personalizados:** Selecione um ou mais grupos com os botões Adicionar e Excluir. Você pode selecionar qualquer um dos grupos personalizados criados, o grupo Alerta, o grupo Conformidade e outros grupos industriais de segurança disponíveis.

Sobre a caixa de diálogo Definições de alerta

Use esta caixa de diálogo para configurar alertas relacionados a segurança, inclusive alertas de vulnerabilidade e de antivírus para dispositivos analisados.

A caixa de diálogo configurações de Alerta contém as seguintes páginas:

Página Definições

Use esta página para configurar alertas de segurança. Se você tiver adicionado definições de segurança ao grupo Alerta, o Patch e Conformidade o alertará sempre que essas definições forem detectadas em um dispositivo analisado.

- **Intervalo mínimo de alerta:** Especifica o intervalo de tempo mais curto (em minutos ou horas) no qual alertas de vulnerabilidades detectadas serão enviados. Você pode usar essas configurações se não desejar ser alertado com muita freqüência. Defina o valor como zero se desejar que os alertas ocorram instantaneamente e em tempo real.
- **Adicionar a um novo grupo Alerta:** Indica quais vulnerabilidades, por nível de gravidade, são colocadas automaticamente no grupo Alerta durante um processo de download de conteúdo. As definições colocadas no grupo Alerta são também colocadas automaticamente no grupo Análise como padrão (a fim de incluir essas definições em uma tarefa de análise de segurança).

Página Antivírus

Use esta página para configurar alertas de antivírus.

- **Nível mínimo de alerta:** Especifica o intervalo mais curto (em minutos ou horas) no qual são enviados os alertas para vírus detectados. Você pode usar essas configurações se não desejar ser alertado com muita freqüência. Defina o valor como zero se desejar que os alertas ocorram instantaneamente e em tempo real.
- **Alerta em:** Indica quais eventos de antivírus geram alertas.

Sobre a caixa de diálogo Definições de núcleo

Use esta caixa de diálogo para habilitar e configurar o envio automático de resultados da última análise de segurança a um servidor núcleo de rollup na sua rede. Análise de dados de segurança permite ver o status de vulnerabilidade em tempo real para todos os dispositivos gerenciados em uma grande rede empresarial distribuída sem ter que carregar manualmente os dados diretamente do servidor núcleo primário.

Sempre que a análise de segurança é executada, ela grava um arquivo de resultados da análise em uma pasta chamada VulscanResults no servidor núcleo e notifica o serviço Web do LANDesk Security Suite que adiciona o arquivo ao banco de dados núcleo. Se as configurações do núcleo de rollup forem habilitadas e um núcleo válido de rollup é identificado, o núcleo de rollup lê o arquivo de resultados da análise em seu banco de dados, fornecendo acesso mais rápido às informações de vulnerabilidade crítica.

Esta caixa de diálogo contém as seguintes opções:

- **Resultados da análise:**
  - **Manter resultados na análise na pasta resultados do vulscan depois de processar:** Salva os arquivos de resultados da análises de segurança na pasta padrão do vulscan.
  - **Descompactar arquivos se necessário:** Habilita a descompactação automática dos arquivos de resultados das análises se estiverem compactados.
- **Contagem do reparo automático:**
  - **Número de tentativas de reparo automático antes de desistir:** Especifique o número de vezes que o servidor núcleo tentará remedia o reparo automático antes de desistir.
  - **Tentar reparo automático indefinidamente:** Indica que o servidor núcleo tentará remediar o reparo automático até conseguir, ou até a interrupção do processo.
- **Núcleo de rollup:**
  - **Enviar resultados da análise ao núcleo de rollup imediatamente:** Habilita o envio imediato dos resultados da análise de segurança ao servidor núcleo especificado, usando o método acima descrito.
  - **Utilizar a URL padrão do rollup:** Marque esta caixa se desejar que a URL padrão seja usada quando o arquivo de resultados da análise for enviado do servidor núcleo para o núcleo de rollup. Insira o nome do servidor núcleo e marque esta caixa para inserir o script e o endereço Web automaticamente no campo **URL do Rollup**.
  - **Núcleo de rollup:** Identifica o núcleo de rollup do qual você deseja receber os últimos resultados de análise de segurança do banco de dados núcleo.
  - **URL do rollup:** especifica o endereço Web do núcleo de rollup que recebe os resultados de análise de segurança e a pasta destino para o arquivo de resultados da análise no núcleo de rollup. O URL do rollup pode ser inserido automaticamente selecionando a caixa de seleção **Utilizar a URL padrão do rollup** ou você pode editar manualmente o campo desmarcando a caixa e inserindo o URL desejado.

Sobre a caixa de diálogo Permissões

Use a caixa de diálogo para exibir as permissões efetivas da ferramenta de Patch e conformidade do administrador atualmente conectado. Essas configurações de permissões são configuradas com a ferramenta Gerenciamento de usuários. Além disso, o LANDesk Administrator pode mudar permissões baseadas em funções requeridos para editar e importar definições personalizadas de vulnerabilidade.

IMPORTANTE: SOMENTE um Administrador da LANDesk pode mudar as permissões baseadas em funções.

Esta caixa de diálogo contém as seguintes opções:

- **Usuário:**
  - **Exibir:** Indica que o usuário pode visualizar o conteúdo segurança de patch.
  - **Editar:** Indica que o usuário pode editar o conteúdo segurança de patch.
  - **Distribuir:** Indica que o usuário pode distribuir o conteúdo segurança de patch.
  - **Editar Público** Indica que o usuário pode editar o conteúdo segurança de patch personalizado.
- **Como interpretar permissões baseadas em funções:**
  - **Requer permissão para Editar público para editar definições personalizadas:** Especifica que a permissão Editar público é exigido para que um usuário seja capaz de editar as definições personalizadas de vulnerabilidade.
  - **Requer permissão Editar público para importar definições:** Especifica que a permissão de Editar público é exigido para que um usuário seja capaz de importar as definições de vulnerabilidade.

Ajuda da barra de ferramentas de Patch e conformidade

Sobre a caixa de diálogo Limpar definições de patch e conformidade

Use esta caixa de diálogo para remover completamente as definições (e suas regras de detecção associadas) do banco de dados núcleo.

IMPORTANTE: Requer direitos de administrador da LANDesk
Um usuário deve possuir permissões de administrador LANDesk para executar esta tarefa.

Remova as definições se elas tiverem se tornado obsoletas e não funcionarem corretamente ou se o risco de segurança relacionado tiver sido totalmente resolvido.

Esta caixa de diálogo contém as seguintes opções:

- **Plataformas:** Especifica as plataformas cujas definições você deseja remover do banco de dados. Se uma definição estiver associada a mais de uma plataforma, você deverá selecionar todas as suas plataformas associadas para que a definição e as informações da regra de detecção sejam removidas.
- **Idiomas:** Especifica as versões de idioma das plataformas selecionadas cujas definições você deseja remover do banco de dados. Se tiver selecionado uma plataforma Windows ou Macintosh, deverá especificar os idiomas cuja definição deseja remover. Se tiver selecionado uma plataforma UNIX ou Linux, deverá especificar a opção Idioma neutro para remover as definições independentes de idioma da plataforma.
- **Tipos:** Selecione os tipos de conteúdo cujas definições você deseja remover.
- **Limpar:** Remove completamente as informações da regra de detecção e a definição para os tipos selecionados que pertencem às plataformas e aos idiomas especificados selecionados. Estas informações só podem ser restauradas se o descarregamento do conteúdo acontecer novamente.
- **Fechar:** Fecha a caixa de diálogo sem salvar as alterações e sem remover as informações de definição.

Sobre tela de informações da análise de segurança

Use esta caixa de diálogo para ver a atividade detalhada da distribuição de patch e o status dos dispositivos na sua rede.

Você pode ver os resultados da análise para:

- Computadores não reportados recentemente
- Computadores sem resultados
- Computadores que precisam de patches pelo tipo de gravidade selecionada

Sobre a caixa de diálogo Definições de limites

Use essa caixa de diálogo para definir os períodos de resultados de análise de segurança (distribuição de patch) que aparecem na caixa de diálogo **Informações da análise de segurança**.

- **Limite para dispositivos não analisados recentemente:** Indica o número máximo de dias para procurar dispositivos que não foram analisados para distribuição de patch.

Sobre a caixa de diálogo Informações de segurança e patch

Use essa caixa de diálogo para exibir informações detalhadas de segurança para os dispositivos selecionados. Você pode ver os resultados de análise de um dispositivo, definições de segurança detectadas, patches instalados ou faltando (ou atualizações de software) e o histórico de reparo.

Use o botão **Limpar** para remover todas as informações de análise do banco de dados para os dispositivos selecionados.

Você pode também clicar com o botão direito em uma vulnerabilidade (ou outro tipo de conteúdo de segurança) nessa tela e criar diretamente uma tarefa de reparo ou habilitar/desabilitar a opção de correção automática para tipos aplicáveis de conteúdo de segurança.

As informações mostradas são baseadas no tipo selecionado do conteúdo de segurança

Os nomes de grupo e campos de informações que são exibidos nesta página são dinâmicos, dependendo do tipo de conteúdo de segurança escolhido na lista suspensa **Tipo**. Por exemplo, se você selecionar vulnerabilidades, os seguintes campos de informação serão exibidos:

- **Patches faltantes (Vulnerabilidades detectadas):** Lista todas as vulnerabilidades detectadas no dispositivo pela última análise.
- **Patches instalados:** Lista todos os patches instalados no dispositivo.
- **Histórico de reparos:** Mostra informações sobre as tarefas de correção tentadas no dispositivo. Estas informações são úteis para a solução de problemas de dispositivos. Para limpar esses dados, clique em **Limpar histórico de reparos**, especifique os dispositivos e as configurações de intervalo de tempo e, em seguida, clique em **Limpar**.
- **Informações de vulnerabilidade:**
  - **Título:** Exibe o título da vulnerabilidade selecionada.
  - **Detectadas:** Indica se a vulnerabilidade selecionada foi detectada.
  - **Primeiramente detectada:** Exibe a data e a hora em que a vulnerabilidade foi inicialmente detectada no dispositivo. Estas informações podem ser úteis se você tiver feito várias análises.

- **Razão:** Descreve o motivo pelo qual a vulnerabilidade selecionada foi detectada. Essas informações podem ser úteis para ajudá-lo a decidir se o risco de segurança é sério o suficiente para uma correção imediata.
- **Esperado:** Exibe o número de versão do arquivo ou da chave do Registro que o analisador de vulnerabilidades está procurando. Se o número de versão do arquivo ou da chave de registro no dispositivo analisado for igual a esse número, não existirá nenhuma vulnerabilidade.
- **Localizado:** Exibe o número de versão do arquivo ou da chave do Registro localizada no dispositivo analisado. Quando esse número é diferente do número Esperado acima, existe uma vulnerabilidade.

- **Informações de correção:**
  - **Correção necessária:** Exibe o nome do arquivo do executável de patch necessário para corrigir a vulnerabilidade selecionada.
  - **Patch instalado:** Indica se o arquivo de patch foi instalado.
  - **Data da última ação:** Exibe a data e a hora em que o patch foi instalado no dispositivo.
  - **Ação:** Indica se a última ação foi uma instalação ou remoção.
  - **Detalhes:** Indica se a distribuição/instalação foi bem-sucedida. Se houver uma falha na instalação, você deverá limpar essas informações de status antes de tentar instalar novamente a correção.
  - **Limpar:** Limpa a data e o status atual da instalação do patch para o dispositivo selecionado. É necessário limpar estas informações para uma nova distribuição e instalação da correção.

Configurações de segurança

Visão geral de Configurações do agente

A nova ferramenta de Configurações de agente fornece uma janela conveniente e única onde você pode criar e gerenciar configurações para vários componentes e serviços LANDesk Security Suite e também tarefas de distribuição correspondentes.

As configurações de agente controlam o modo como os serviços de segurança operam em dispositivos gerenciados. Os serviços de segurança e suas configurações associadas podem ser distribuídas para os dispositivos gerenciados como parte da configuração de agente inicial, instalação separada ou tarefas de atualização e tarefas de configurações mudanças.

As Configurações de agente permitem criar e gerenciar configurações para os seguintes serviços de segurança:

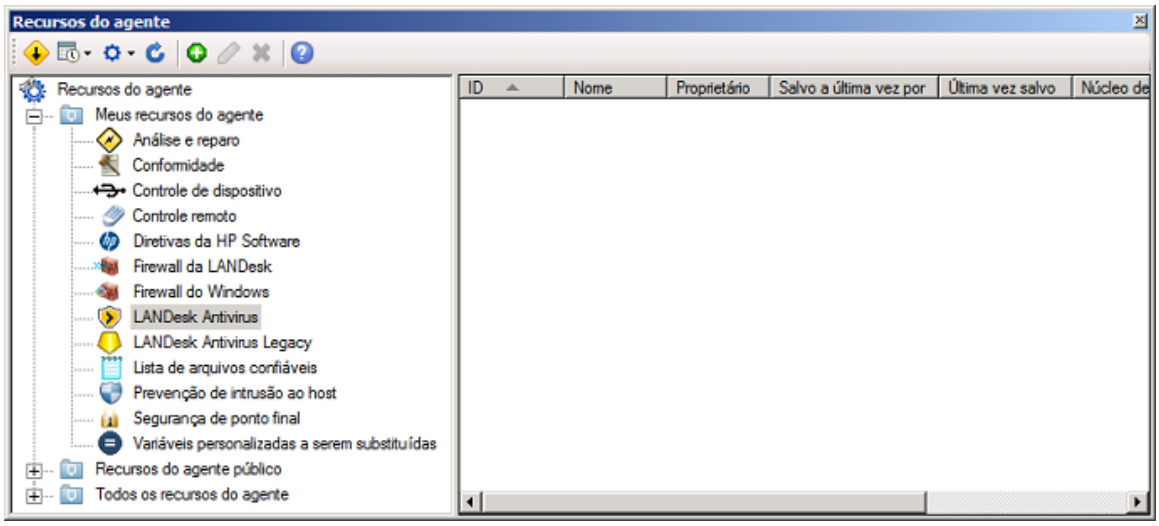
- Conformidade
- Variáveis personalizadas a serem substituídas
- Controle de dispositivo
- Firewall do Windows
- Segurança de ponto final (HIPS, LANDesk Firewall e Controle de dispositivo)
- Prevenção de intrusão no host
- Diretivas da HP Software
- LANDesk Antivirus
- LANDesk Antivirus Legacy
- LANDesk Firewall
- Controle remoto
- Análise e reparo
- Listas de arquivos confiáveis
- Firewall do Windows

Você também pode realizar as tarefas de segurança de componentes descritas neste capítulo.

IMPORTANTE: Permissões de grupos LANDesk Script Writers são necessárias
Para criar tarefas agendadas e diretivas na ferramenta Patch e conformidade e a ferramenta Configurações de segurança (para tarefas de análise de segurança e conformidade, tarefas de reparo e tarefas de mudanças de configurações), um usuário precisa ter permissão de grupo LANDesk Script Writers. Em outras palavras, eles precisam pertencer a um grupo que tenha permissão de LANDesk Script Writers atribuída. Para obter mais informações sobre a administração baseada em funções, consulte "Gerenciamento de usuários" na página 38.

Configurar tarefas e parâmetros de segurança

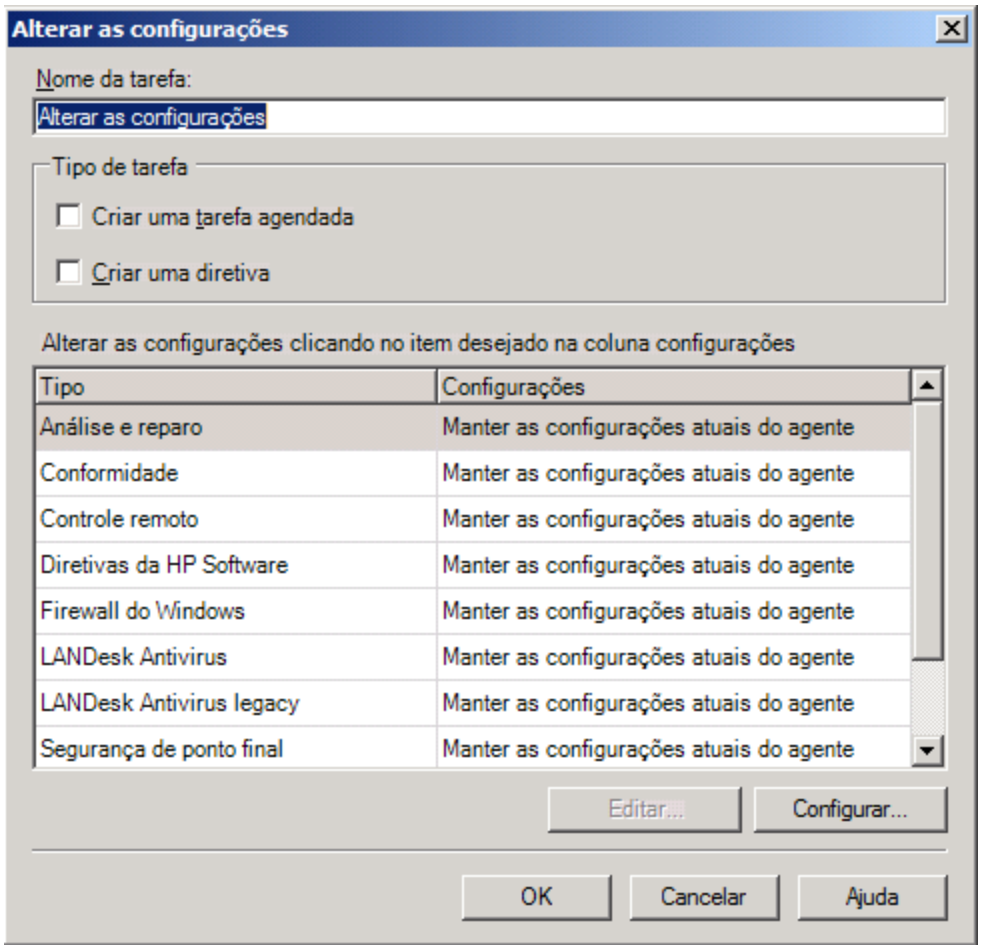
A janela da ferramenta Configurações de agente fornece uma interface única conveniente que permite gerenciar parâmetros e tarefas para vários serviços e componentes de segurança.



Criar tarefas de configurações de mudança

As configurações de segurança padrão de dispositivo são distribuídas como parte da configuração inicial do agente. Em algum momento, você pode precisar mudar essas configurações padrão em determinados dispositivos. A ferramenta Configurações de agente fornece um meio de fazer isso sem ter que redistribuir uma configuração de agente nova e completa.

Para fazer isso, clique na tarefa **Mudar configurações** localizada no botão **Criar uma tarefa** da barra de tarefas.



A caixa de diálogo que é exibida permite digitar um nome exclusivo para a tarefa, especificar se é uma tarefa agendada ou uma diretiva e selecionar a configuração existente como padrão ou usar o botão Editar para criar a nova configuração padrão dos dispositivos alvo.

Ajuda sobre mudar configurações

Sobre a caixa de diálogo Criar tarefa de alteração de configurações

Use esta caixa de diálogo para criar e configurar uma tarefa que muda as configurações padrão para componentes de Segurança de ponto final.

Com uma tarefa de alteração de configurações, você pode alterar de forma conveniente as configurações padrão do dispositivo gerenciado (gravadas no Registro local do dispositivo) sem a necessidade de redistribuir uma configuração completa de agente.

Esta caixa de diálogo contém as seguintes opções:

- **Nome da tarefa:** Digite um nome exclusivo para identificar a tarefa.
- **Criar uma tarefa agendada:** Adiciona a tarefa à janela Tarefas agendada, onde você pode configurar as suas opções de agendamento e recorrência, além de designar dispositivos alvo.
- **Criar uma diretiva:** Adicione a tarefa como uma diretiva à janela Tarefas agendadas onde você pode configurar as opções da diretiva.

- **Tipo:** identifica o componente de segurança.
- **Segurança de ponto final:** especifica as configurações de Segurança de ponto final associadas a esta tarefa de mudança de configurações em particular. Lembre-se que embora a Segurança de ponto final seja um agente único que é distribuído para dispositivos alvo, ele fornece serviços para vários componentes de segurança,incluindo Alerta ao local (conexões de rede), HIPS, LANDesk Firewall e Controle de dispositivo. Selecione as configurações que deseja distribuir para os dispositivos alvo, modifique a configuração existente selecionando-as e clicando em **Editar** ou crie uma nova configuração clicando em **Configurar > Nova**.
- **Antivírus:** Especifica as configurações de antivírus usadas para as tarefas de análise antivírus. Configurações de antivírus determinam se o ícone LANDesk Antivirus aparece na bandeja do sistema do dispositivo, disponibilidade de opções interativas para usuários finais, verificação de e-mail e ativação de proteção em tempo real, tipos de arquivos para verificar, arquivos e pastas para excluir, quarentena de arquivo infectado e Backup, verificação agendada de antivírus, e definições de atualizações de vírus agendados. Selecione uma das definições na lista. Clique em **Editar** para modificar as opções das definições selecionadas. Clique em **Configurar** para criar novas definições. Para encontrar mais informações, consulte a "Sobre a caixa de diálogo Configurações do LANDesk Antivirus" na página 741.
- **Firewall do Windows:** Especifique as configurações de firewall do Windows em dispositivos alvo. Você pode habilitar/desabilitar o firewall e configurar definições de firewall incluindo exceções, regras de entrada e de saída (para serviços, portas, programas).

Sobre a caixa de diálogo Configurar parâmetros do componente de segurança

Use esta caixa de diálogo para gerenciar suas configurações. Esta caixa de diálogo é compartilhada por vários componentes de segurança porque inclui opções comuns de controle.

Uma vez configuradas, você pode aplicar as configurações às tarefas de configuração do agente, tarefas de instalação ou atualização de componentes de segurança e a tarefas de mudança de configurações.

Esta caixa de diálogo contém as seguintes opções:

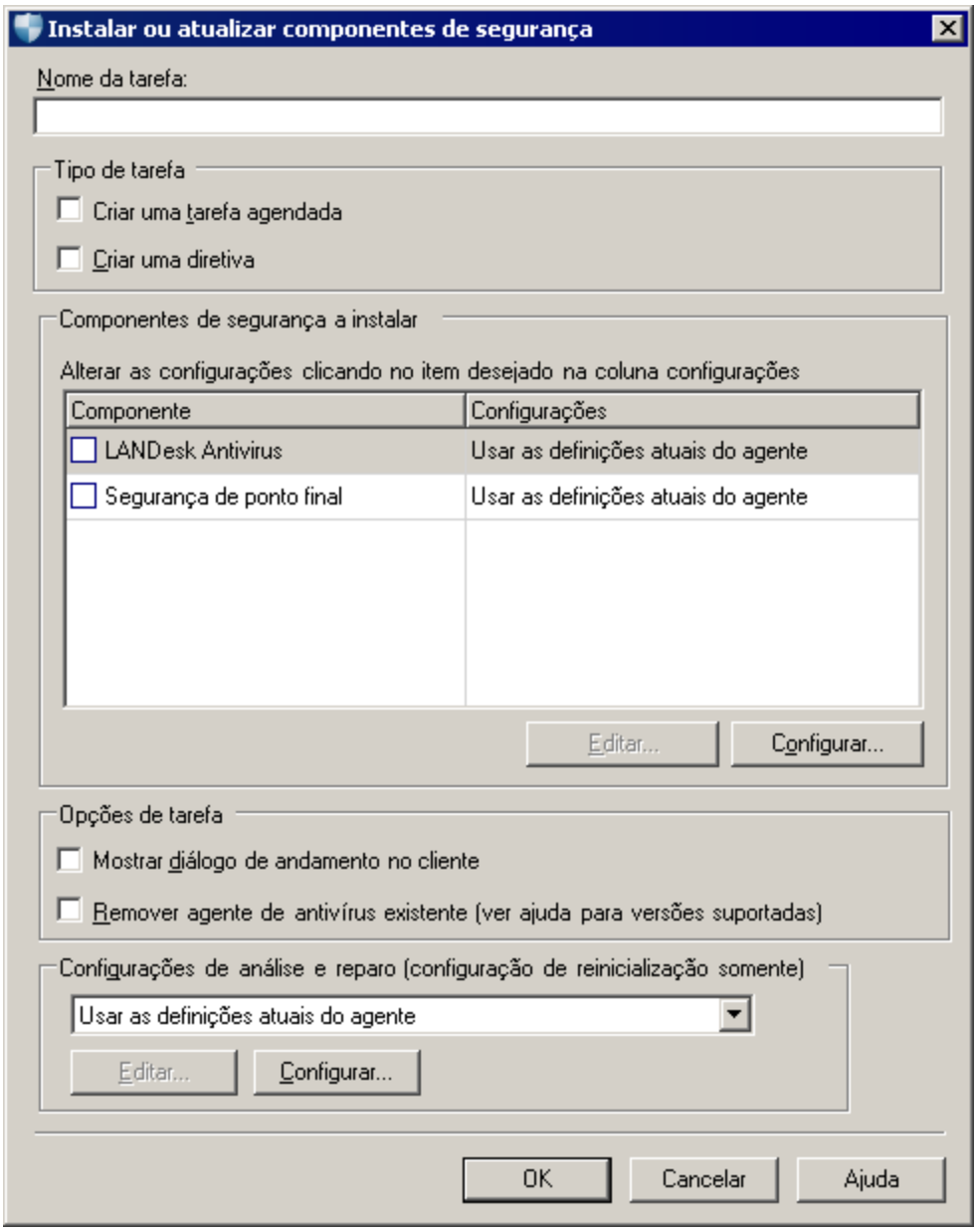
- **Novo:** Abre a caixa de diálogo de configurações onde você pode configurar várias opções.
- **Editar:** Abre a caixa de diálogo de definições onde você pode modificar a configurações selecionadas.
- **Copiar:** Abre uma cópia das configurações selecionadas como um modelo que pode ser modificado e renomeado. Isso é útil quando você deseja fazer pequenos ajustes nas configurações e salvá-los para um fim específico.
- **Excluir:** remove as configurações selecionadas do banco de dados. (Observe que as configurações selecionadas pode estar associada no momento com uma ou mais tarefas ou dispositivos gerenciados. Se você decidir excluir a configuração: dispositivos com aquelas definições ainda a reterão e continuarão a usá-las até que uma nova tarefa de mudança de configurações seja distribuída; as tarefas agendadas com aquelas configurações ainda serão executadas nos dispositivos alvo, assim como as tarefas do agendador local com aquelas configurações até que uma nova configuração seja distribuída.
- **Usar selecionada:** Indica que as configurações selecionadas atuais serão usada para a tarefa.
- **Fechar:** Fecha a caixa de diálogo sem aplicar nenhuma configuração à tarefa.

Criar uma tarefa para instalar ou atualizar componentes de segurança

Se você desejar instalar ou atualizar componentes de segurança, você pode fazer isso como uma tarefa separada.

Para criar uma tarefa de instalação ou atualização de componentes de segurança

1. No console, clique em **Ferramentas > Segurança e Conformidade > Configurações de agente**.
2. Clique no botão **Criar uma tarefa** da barra de ferramentas e clique em **Instalar ou atualizar os componentes de segurança**.



3. Digite um nome para a tarefa.
4. Especifique se a instalação é uma tarefa agendada, baseada em diretivas ou ambas.
5. Selecione o componente que deseja instalar. Você pode criar novas configurações ou editar as configurações existentes clicando em **Configurar**.
6. Para mostrar o andamento da instalação na caixa de diálogo do analisador de segurança nos dispositivos alvo, selecione a opção **Mostrar diálogo de andamento no cliente**.
7. Selecione uma configuração de análise e reparo na lista para aplicar sua configuração de reinicialização (somente) à configuração de agente que está criando. Você pode criar novas configurações ou editar as configurações existentes clicando em **Configurar**. Tenha em mente que *somente as opções de reinicialização* especificadas nas configurações de análise e reparo que você selecionou são usadas na distribuição do agente de Segurança de ponto final para dispositivos alvo desta configuração de agente. É possível usar as configurações de análise e reparo que já incluam a configuração de reinicialização desejada ou criar novas configurações, específicas para o seu agente de distribuição.
8. Clique em **OK**.

Ajuda do Instalar ou atualizar componentes de segurança

Sobre a caixa de diálogo Tarefa de instalação ou atualização de componentes de segurança

Use esta caixa de diálogo para criar e configurar uma tarefa que instala os componentes de segurança (atra'ves do agente de segurança de ponto final) nos dispositivos alvo em que ele ainda não foi instalado ou que atualiza a versão existente dos componentes de segurança nos dispositivos alvo.

NOTA: A instalação é executada pelo analisador de segurança.

Essa tarefa permite a distribuição e atualização convenientes de componentes de segurança de um dispositivo gerenciado (e das configurações associadas) no dispositivo gerenciado sem que seja necessário redistribuir uma configuração de agente completa.

Esta caixa de diálogo contém as seguintes opções:

- **Nome da tarefa:** Digite um nome exclusivo para identificar a tarefa.
- **Criar uma tarefa agendada:** Adiciona a tarefa à janela Tarefas agendada, onde você pode configurar as suas opções de agendamento e recorrência, além de designar dispositivos alvo.
- **Criar uma diretiva:** Adicione a tarefa como uma diretiva à janela Tarefas agendadas onde você pode configurar as opções da diretiva.
- **Componentes a serem a instalar:** Especifica que componentes de segurança serão instalados com a tarefa. Marque o componente que deseja instalar. Clique na coluna **Configurações** para selecionar as configurações existentes. Clique em **Editar** para modificar as opções das definições selecionadas. Clique em **Configurar** para criar novas definições.
- **Mostrar diálogo de andamento no cliente:** Indica se a caixa de diálogo do analisador de segurança mostra o andamento da instalação nos dispositivos alvo.

- **Remover agente existente de antivírus:** Remove automaticamente outro software antivírus que possa já estar instalado nos dispositivos antes da instalação do LANDesk Antivirus (veja abaixo). (**NOTA:** É também possível escolher a remoção de software existente de antivírus dos dispositivos gerenciados durante uma configuração inicial de agente.)
- **Configurações de análise e reparo (reinicialização somente):** Especifica as configurações de análise e reparo associadas a esta instalação em particular. A tarefa usará as opções de reinicialização das configurações de análise e reparo SOMENTE, o que determina os requisitos de reinicialização e as ações nos dispositivos alvo durante a instalação.

Lista de produtos antivírus de terceiros que podem ser removidos automaticamente

Para a lista atual na seção principal do LANDesk Antivirus, consulte "LANDesk Antivirus" na página 712.

Criar uma tarefa para remover componentes de segurança

Se desejar remover os componentes de segurança dos dispositivos gerenciados, você também poderá fazê-lo como uma tarefa do console.

Para criar uma tarefa de remoção de componentes de segurança

1. No console, clique em **Ferramentas > Segurança e Conformidade > Configurações de agente**.
2. Clique no botão **Criar uma tarefa** da barra de ferramentas e clique em **Remover componentes de segurança**.
3. Digite um nome para a tarefa.
4. Especifique se a instalação é uma tarefa agendada, baseada em diretivas ou ambas.
5. Selecione o componente que deseja remover.
6. Para mostrar o andamento da instalação na caixa de diálogo do analisador de segurança nos dispositivos alvo, selecione a opção **Mostrar diálogo de andamento no cliente**.
7. Selecione uma configuração de análise e reparo na lista disponível para aplicar sua configuração de reinicialização à tarefa que está criando. Você pode criar novas configurações ou editar as configurações existentes clicando em **Configurar**. A tarefa usará as opções de reinicialização das configurações de análise e reparo SOMENTE, o que determina os requisitos de reinicialização e as ações nos dispositivos alvo durante a remoção do agente.
8. Clique em **OK**.

Ajuda do Remover componentes de segurança

Sobre a caixa de diálogo da tarefa Remover componentes de segurança

Use esta caixa de diálogo para criar e configurar uma tarefa que remove os componentes de segurança dos dispositivos alvo.

Esta caixa de diálogo contém as seguintes opções:

- **Nome da tarefa:** Digite um nome exclusivo para identificar a tarefa.
- **Criar uma tarefa agendada:** Adiciona a tarefa à janela Tarefas agendada, onde você pode configurar as suas opções de agendamento e recorrência, além de designar dispositivos alvo.

- **Criar uma diretiva:** Adicione a tarefa como uma diretiva à janela Tarefas agendadas onde você pode configurar as opções da diretiva.
- **Componentes de segurança a remover:** Especifica que componentes de segurança serão removidos com a tarefa. Selecione o componente que deseja remover.
- **Mostrar diálogo de andamento no cliente:** indica se a caixa de diálogo do analisador de segurança mostra o andamento da remoção do agente dos dispositivos alvo.
- **Configurações de análise e reparo (reinicialização somente):** especifica as configurações de análise e reparo associadas a esta tarefa de remoção em particular de agente. A tarefa usará as opções de reinicialização das configurações de análise e reparo SOMENTE, o que determina os requisitos de reinicialização e as ações nos dispositivos alvo durante a remoção do agente.

Ajuda das Listas de arquivos confiáveis

Sobre a caixa de diálogo Lista de arquivos confiáveis

Use este diálogo para gerenciar suas configurações. Listas de arquivos confiáveis são compostas de arquivos com um conjunto de permissões específicas (privilégios ou autorizações) que permitem e negam determinadas ações que podem ser executadas naquele arquivo *por* um aplicativo.

Esta caixa de diálogo contém as seguintes opções:

- **Nome:** Identifica a lista de arquivos confiáveis com um nome exclusivo. Você pode usar o recurso **Localizar** permite que você pesquise itens em uma lista que contenha uma palavra ou expressão específica. A lista resultante exibe apenas os itens que correspondem aos seus critérios de pesquisa.
- **Adicionar:** abre uma caixa de diálogo do Explorer que permite procurar e selecionar um arquivo para configurar com as certificações de arquivos.
- **Editar:** permite selecionar as certificações do arquivo selecionado.
- **Excluir:** exclui o arquivo selecionado e suas certificações.
- **Mover:** Abre uma caixa de diálogo que permite que você selecione uma ou mais lista de arquivos confiáveis e ou movê-los ou copiá-los para outra lista.
- **Definir como padrão:** Atribui esta lista como a lista de arquivos confiáveis padrão para tarefas que usem esta configuração HIPS (ou Firewall).
- **ID:** Identifica esta lista específica. Esta informação é armazenada no banco de dados e pode ser usada para controlar cada uma das listas.

Sobre a caixa de diálogo Arquivo confiável

Use esta caixa de diálogo para configurar as permissões HIPS e/ou LANDesk Firewall para um arquivo específico.

Esta caixa de diálogo contém as seguintes opções:

- **Nome do arquivo:** identifica o arquivo de aplicativo ao qual as certificações estão sendo atribuídas.
- **Caminho completo:** especifica o local do arquivo.
- **Tamanho do arquivo:** especifica o tamanho (em KB) do arquivo.
- **Data do arquivo:** indica a data e a hora de criação do arquivo.
- **Versão:** indica o número da versão do arquivo, se houver.
- **Certificado:** indica a data e a hora em que as certificações do arquivo foram criadas ou modificadas pela última vez.

- **Hash MD5:** mostra o hash MD5 do arquivo. Um arquivo de hash é usado para garantir a integridade do arquivo.
- **Descrição:** uma caixa de texto que permite inserir uma descrição para o arquivo.
- **Ignorar toda a proteção:** permite que o arquivo de aplicativo complete os privilégios. O arquivo não será filtrado ou monitorado.
- **Ignorar proteção contra estouro de buffer:** Permite ignorar a proteção contra estouro de buffer. Você poe usar essa opção com arquivos (processo) que estão certificados e são de sua confiança.
- **Segurança do sistema**
  - **Modificar arquivos executáveis:** concede ao aplicativo o direito de modificar outros arquivos executáveis.
  - **Modificar arquivos protegidos:** concede ao aplicativo o direito de modificar arquivos protegidos. Você pode gerar uma lista de arquivos protegidos, como de agentes de dispositivos LANDesk Management Suite.
  - **Modificar chaves do Registro protegidas:** concede ao aplicativo o direito de modificar chaves do registro protegidas. As chaves protegidas impedem as infecções por malware.
- **Segurança de rede**
  - **Enviar emails:** permite que o aplicativo envie mensagens de email. (**NOTA:** O HIPS reconhece os aplicativos clientes de email padrão e os certifica automaticamente para que possam enviar emails.)
- **Arquivos no disco**
  - **Adicionar à inicialização do sistema:** concede ao aplicativo o direito de adicionar arquivos à inicialização do sistema.
  - **Permitir execução:** permite que o aplicativo (processo) execute no dispositivo. A execução de arquivos certificados é habilitada automaticamente. E, se uma certificação de arquivo fornecer direitos parciais, então a permissão da opção de execução é automaticamente habilitada.
- **Regras de segurança avançadas**
  - **Proteger aplicativo na memória:** impõe proteção para o aplicativo que está sendo executado na memória. O aplicativo é protegido contra término ou modificação.
  - **Herdar para os processos filhos:** atribui as mesmas certificações (direitos) de arquivos a todos os processos subordinados executados por este aplicativo. Por exemplo, você pode aplicá-la a um executável de instalação para passar os mesmos direitos para os processos subseqüentes iniciados pelo programa de instalação.
  - **Instalador autorizado:** Indica que o aplicativo possui permissão para executar a instalação ou distribuição de software. Esse é o caso da ferramenta de distribuição de software do LANDesk Management Suite e pode também ser aplicável a outros aplicativos de distribuição de software.
- **Opções de aprendizado**
  - **Travar certificação de arquivo (autorizações não serão atualizadas através do modo de aprendizagem):**
  - **Corresponder esta entrada com base somente no nome do arquivo:**
- **OK:** Salva as certificações e as adiciona à lista de arquivos certificados na caixa de diálogo Configurações do HIPS.
- **Cancelar:** fecha a caixa de diálogo sem salvar as certificações.

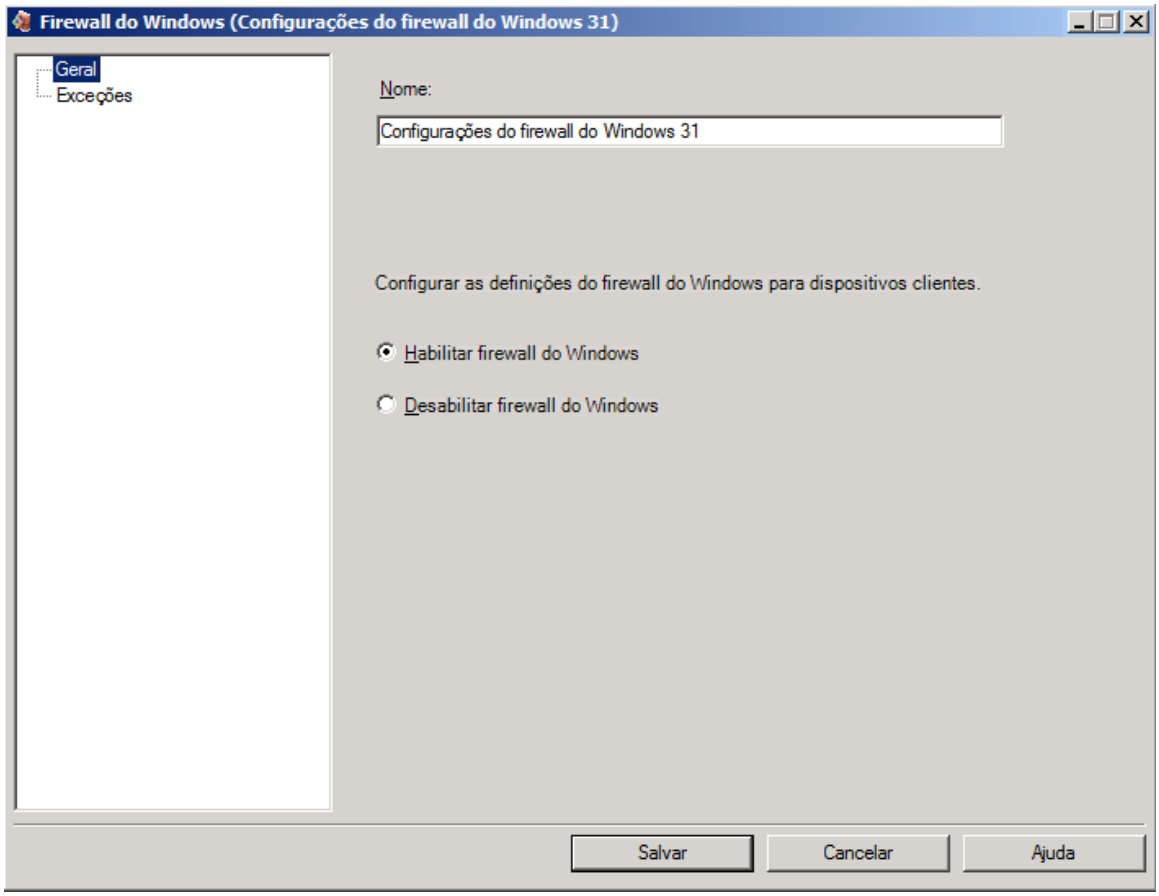
Tópicos relacionados

Configurar as definições do firewall do Windows

A ferramenta de Configurações de agente permite também criar, configurar e distribuir as configurações de firewall do Windows para gerenciar o firewall do Windows nos dispositivos alvo.

Para criar as configurações do LANDesk Firewall

1. Clique em **Ferramentas > Segurança e Conformidade > Configurações de agente**.
2. Clique com o botão direito em **Firewall do Windows**, clique em **Novo**, selecione a plataforma desejada do Windows e clique em **OK**.



Uma vez configuradas, você poderá distribuir as configurações para dispositivos alvo com uma tarefa de instalação ou de atualização ou uma tarefa de mudança de configurações.

Ajuda do Firewall do Windows

Sobre a caixa de diálogo Configurar parâmetros de firewall do Windows

Use esta caixa de diálogo para configurar os parâmetros de firewall do Windows. As configurações de firewall Windows são associadas a uma tarefa de mudança de configurações para habilitar/desabilitar a firewall e configurar os parâmetros de firewall que incluem exceções, regras de entrada e regras de saída (para serviços, portas e programas).

É possível usar esse recurso para distribuir uma configuração para o firewall Windows nas seguintes versões do Windows:

- Windows 2003
- Windows XP (SP2 ou mais recente)
- Windows Vista

Sobre a Firewall do Windows (XP/2003): Página geral

Use esta página para definir as configurações geris de firewall.

Sobre a Firewall do Windows (XP/2003): Página Exceções

Use esta página para configurar exceções de firewall.

Esta caixa de diálogo contém as seguintes opções:

- **Exceções atuais:** Lista os programas, portas e serviços cuja conexão/comunicação *não* está sendo bloqueada pelo firewall. O firewall impede o acesso não autorizado a dispositivos, com exceção dos itens desta lista.
- **Adicionar programa:** Permite adicionar um programa específico à lista de exceções para permitir a comunicação.
- **Adicionar porta:** Permite adicionar uma porta específica à lista de exceções para permitir a comunicação.
- **Editar:** Permite a edição das propriedades das exceções selecionadas, inclusive o escopo dos dispositivos afetados.
- **Excluir:** Remove a exceção selecionada da lista.
- **OK:** Salva as alterações e fecha a caixa de diálogo.
- **Cancelar:** Fecha a caixa de diálogo sem salvar as alterações.

Definições dos riscos de segurança do firewall do Windows

Além disso, o LANDesk Security Suite fornece definições de risco de segurança pré-definidas que lhe permitem analisar, detectar e configurar parâmetros de firewall em dispositivos gerenciados que executam plataformas Windows específicas. As seguintes definições de ameaça de segurança permitem que você faça uma análise em busca de e modifique as configurações de firewall:

- **ST000102:** Definição de ameaça de segurança para a firewall do Windows no Windows 2003 e Windows XP.
- **ST000015:** Definição de ameaça de segurança para Firewall de conexão de Internet no Windows 2003 e Windows XP.

As propriedades dos riscos de segurança do firewall do Windows incluem variáveis personalizadas que permitem a configuração dos parâmetros do firewall do Windows. Você pode usar essas definições de ameaça de segurança para analisar e procurar parâmetros especificados e retornar uma condição de vulnerabilidade se esses parâmetros não forem correspondidos. Use, então, a definição personalizada em uma tarefa de reparo para ativar ou desativar a firewall e mudar ou reconfigurar os parâmetros da firewall no dispositivo analisados.

Sobre a página Firewall do Windows (Vista): Página de regras gerais

Use esta página para configurar as regras geralis de firewall.

Sobre a página Firewall do Windows (Vista): Regras de entrada

Use esta página para configurar as regras de entrada de firewall.

Sobre a página Firewall do Windows (Vista): Regras de saída

Use esta página para configurar as regras de saída de firewall.

Gerar códigos de autorização de segurança

Use esta caixa de diálogo para criar um código de autorização que permitirá que um usuário final execute uma operação bloqueada por um curto período. Você pode usar um código de autorização para fornecer acesso temporário para um usuário específico ou para um administrador de TI para ter acesso a um dispositivo gerenciado.

Por exemplo, se um usuário tentar conectar um dispositivo USB que não é permitido por configurações de Controle de dispositivo, uma mensagem pop-up será exibida no dispositivo do usuário final que inclui um código de operação. O usuário deve fornecer o código de operação ao administrador que o utiliza para gerar um código de autorização, o qual é dado ao usuário final. Isto permite que o usuário execute a ação temporariamente.

Para gerar um código de autorização

1. Na janela da ferramenta do **Configurações de agente**, clique no botão **Configurações comuns** da barra de ferramentas e, em seguida, clique em **Gerar código de autorização**.
2. Digite o código de operação fornecido pelo usuário final.
3. Se o código de operação for válido, é gerado um código de autorização automaticamente.
4. Digite o tipo de operação que o usuário final deseja realizar.
5. Fornecer o código de autorização ao usuário final. O usuário insere o código de autorização quando solicitado para realizar a operação bloqueada.

CUIDADO: Mensagem pop-up imprecisa
Quando um usuário recebe acesso através de um código de autorização, uma mensagem pop-up pode aparecer no dispositivo do usuário final indicando que o HIPS foi desativado independentemente da ação executada pelo usuário. Essa mensagem pode ser ignorada.

Atividade da segurança

Visão geral da Atividade de segurança

A nova ferramenta **Atividade de segurança** fornece uma conveniente janela única onde você pode ver as informações de status e atividade de vários serviços do LANDesk Security Suite em execução nos dispositivos gerenciados.

A Atividade de segurança permite ver informações de status e atividade para:

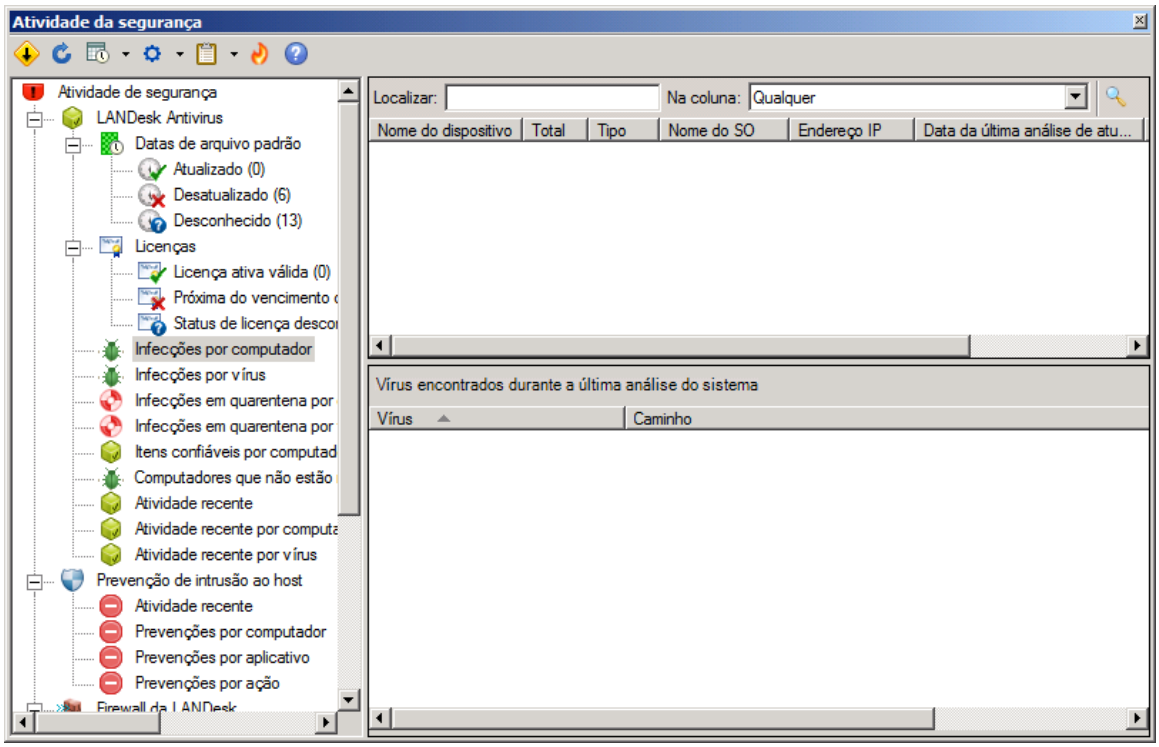
- LANDesk Antivirus
- Host Intrusion Prevention (HIPS)
- LANDesk Firewall
- Controle de dispositivo

Você pode também executar essas tarefas:

- Configurar parâmetros de limites de atividade de segurança
- Depurar informações de atividade de segurança

Exibir status e atividade de segurança

A ferramenta Atividade de segurança permite ver informações sobre serviços do LANDesk Security Suite.



As ferramentas de segurança que você pode ver são descritas nas seguintes seções.

Exibir a atividade e informações de status do LANDesk Antivirus

Se o analisador do LANDesk Antivirus descobrir uma das definições selecionadas de vírus nos dispositivos alvo, essa informação é reportada ao servidor núcleo. Você pode usar qualquer um dos métodos abaixo para exibir dados de segurança detectados após executar uma análise.

Esta janela mostra a atividade de antivírus e as informações de status pelas seguintes categorias:

- Infecções por computador
- Infecções por vírus
- Infecções em quarentena por computador
- Infecções em quarentena por vírus
- Itens confiáveis por computador
- Computadores que não informaram atividade de antivírus recentemente
- Atividade recente de antivírus por computador
- Atividade recente de antivírus por vírus

Além disso, nos dispositivos analisados, clique com o botão direito no dispositivo, selecione **Informações de Segurança e patch** e, na lista suspensa **Tipo**, selecione **Antivírus**. É possível ver:

- Atualizações de antivírus ausentes
- Atualizações de antivírus instaladas
- Depurar histórico de reparo

Sobre a caixa de diálogo Informações sobre atividades e status do antivírus

Use esta caixa de diálogo para ver em detalhes a atividade e o status de todos os dispositivos gerenciados com o agente do LANDesk Antivirus. Essa análise fornece dados que são usados para gerar os relatórios LANDesk Antivirus disponíveis na ferramenta **Relatórios**.

Para personalizar o escopo e foco de dados mostrados, clique em **Limites** e mude os limites de tempo para a recente atividade de antivírus do dispositivo analisado e dispositivos que não tiverem sido analisados recentemente.

Também é possível clicar com o botão direito em um dispositivo nessa tela para acessar o menu de atalho e executar diretamente as tarefas disponíveis.

Esta caixa de diálogo contém as seguintes opções:

- **Atualizar:** Atualiza os campos na caixa de diálogo com as últimas informações de análise antivírus do banco de dados.
- **Limites:** Abre a caixa de diálogo **Definições de limites**, onde você pode definir a duração (em dias) da recente atividade de antivírus e da análise antivírus "não recente". Os limites determinam o período de tempo para o qual os resultados de análise antivírus são organizados e mostrados para as duas categorias de tela específicas de computador.
- **Infecções por computador:** Mostra dispositivos no painel direito nos quais foram descobertas infecções de vírus durante a última análise do sistema. Selecione um dispositivo para ver seus vírus específicos.
- **Infecções por vírus:** Mostra vírus no painel direito descobertos em dispositivos gerenciados durante a última análise do sistema. Selecione uma definição de vírus para ver os dispositivos infectados.

- **Computadores que não foram analisados recentemente para detecção de vulnerabilidades de antivírus:** Mostra todos os dispositivos com o agente do LANDesk Antivirus que não foram analisados para detecção de vírus no período especificado na caixa de diálogo **Definições de limites**. Para executar uma análise imediata de antivírus, clique com o botão direito no dispositivo, clique em **Iniciar tarefa de análise LANDesk Antivirus agora**, selecione uma definição de antivírus e clique em **OK**.
- **Computadores com atividade recente de antivírus:** Mostra todos os dispositivos com o agente do LANDesk Antivirus que foram analisados e mostraram uma atividade de antivírus no período especificado na caixa de diálogo **Definições de limites**. Selecione um dispositivo para visualizar suas atividades específicas de antivírus, incluindo detecção de vírus, remoção, quarentena de objeto infectado, backup e restauração.

Exibir atividade do HIPS

Se o HIPS detectar violações de suas regras e direitos de certificação, essas informações serão relatadas para o servidor núcleo. Você poderá usar os métodos a seguir para exibir a atividade detectada do HIPS.

Para obter informações sobre a atividade HIPS em sua rede, na ferramenta Atividade de segurança, abra o grupo **Intrusão do host**. A janela exibe a atividade do HIPS pelas seguintes categorias:

- Prevenções por computador
- Prevenções por aplicativo
- Prevenções por ação

Você também pode exibir atividades de intrusão de hosts específicos na parte inferior da janela, incluindo os seguintes detalhes:

- Data da ação
- Ação
- Descrição
- Aplicativo
- Versão do arquivo
- Tamanho do arquivo
- Data do arquivo
- Modo
- Hash MD5

Sobre a caixa de diálogo de Atividade do HIPS

Use esta caixa de diálogo para ver em detalhes as atividades do HIPS de todos os dispositivos gerenciados com o agente do LANDesk HIPS. Esses dados são usados para gerar os relatórios do LANDesk HIPS disponíveis na ferramenta **Relatórios**.

Para personalizar o escopo e o foco dos dados exibidos, clique em **Limites** e altere o limite de período de tempo para o armazenamento de informações de atividade do HIPS no banco de dados núcleo e para o número de itens a serem exibidos nas listas de atividade do HIPS.

Também é possível clicar com o botão direito em um dispositivo nessa tela para acessar o menu de atalho e executar diretamente as tarefas disponíveis.

Esta caixa de diálogo contém as seguintes opções:

- **Atualizar:** Atualiza os campos na caixa de diálogo com as últimas informações do HIPS existentes no banco de dados.
- **Limites:** Abre a caixa de diálogo **Configurações do limites**, a qual permite definir a duração (em dias) do armazenamento dos dados do HIPS no banco de dados e o número de itens a serem exibidos nas listas de atividades do HIPS.
- **Limpar:** remove de forma completa e permanente os dados de atividades do HIPS desta janela de exibição e do banco de dados núcleo.
- **Prevenções por computador:** lista os dispositivos no painel direito no qual violações de HIPS foram descobertas. Selecione um dispositivo para consultar violações específicas.
- **Prevenções por aplicativo:** lista os aplicativos no painel direito que foram descobertos nos dispositivos gerenciados. Selecione um aplicativo para ver os dispositivos nos quais ele foi descoberto.
- **Prevenções por ação:** lista as ações no painel direito que foram executadas nos dispositivos gerenciados. Selecione uma ação para ver os dispositivos nos quais ela foi executada.

Exibir atividade LANDesk Firewall

A janela exibe a atividade de Firewall pelas seguintes categorias:

- Prevenções por computador
- Prevenções por aplicativo
- Prevenções por ação

Exibe a atividade de Controle de dispositivo

A janela exibe a atividade de Controle de dispositivo pelas seguintes categorias:

- Dispositivos de armazenamento bloqueados
- Dispositivo CD/DVD bloqueado
- Outros dispositivos bloqueados
- Arquivos de cópia sombra

Configurar parâmetros de limites de atividade de segurança

Security activity information for your managed devices can build up quickly and adversely impact the performance of the core database.

Use this dialog box to define data collection time periods and control the amount of security-related data that is stored in the core database for the LANDesk Antivirus, HIPS, and Firewall tools. 7This information appears in the corresponding Security Activity views.

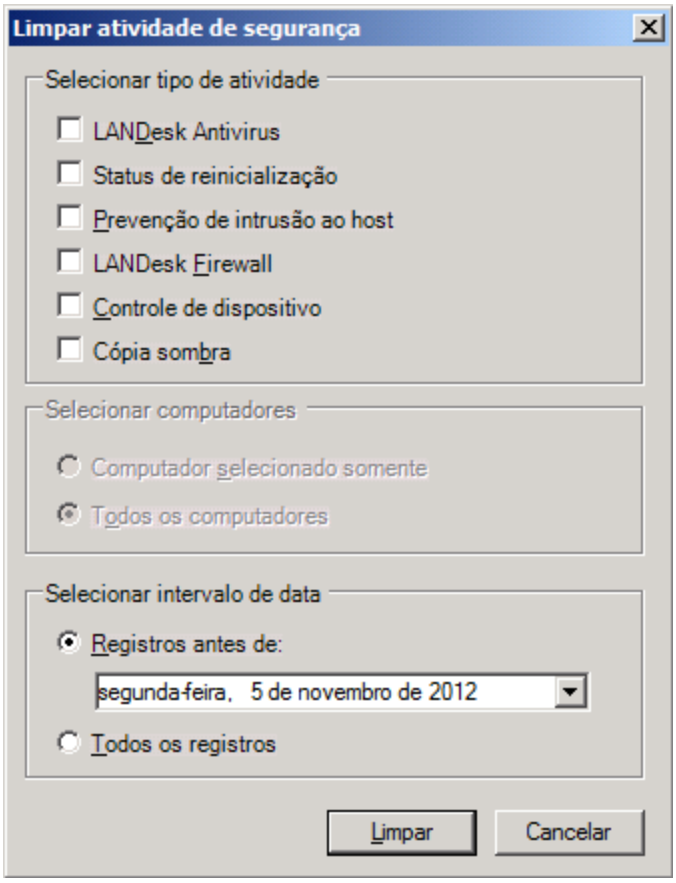
Sobre a caixa de diálogo Definições de limites

- **Tendências comuns:**
  - **Limite para exibição de atividades recentes:** Especifica o período (em dias) para coletar atividades de antivírus para dispositivos que foram analisados e retornaram atividades de antivírus.
  - **Ao exibir os resultados, truncar as listas para:** indica o número máximo de entradas a serem exibidas nas listas nos diálogos de atividade. É possível especificar de 1 a 999.999 itens.

- **LANDesk Antivirus:**
  - **Arquivos padrão desatualizados se mais velhos que:**
  - **Aviso de limite da validade da licença:**
  - **Limite para os que não foram analisados recentemente:** Especifica o período (em dias) para coletar informações de dispositivo para todos os dispositivos configurados com antivírus que não foram analisados.
- **Purgação automática (HIPS / somente Firewall da LANDesk):**
  - **Excluir automaticamente atividades anteriores a:** Indica o número máximo de dias durante os quais as atividades do HIPS e do LANDesk Firewall relatadas para os dispositivos protegidos serão mantidas no banco de dados núcleo. É possível especificar de 1 a 999 dias. **(IMPORTANTE:** A LANDesk recomenda que você observe com cuidado a quantidade de dados que é enviada para o núcleo e encontre um número de dias adequado para que os dados do HIPS não usem muito espaço ou afetem o desempenho do banco de dados do núcleo.)

Limpar atividade de segurança

De vez em quando você pode precisar depurar informações de atividades de segurança para vários componentes de segurança. Isso pode ser feito com o botão **Depurar atividades** da barra de ferramenta em Atividade de segurança.



Purgação de atividade de segurança é uma tarefa única e não uma tarefa agendada ou uma diretiva.

Sobre a caixa de diálogo Depurar atividades de segurança

Use esta caixa de diálogo para remover completamente os registros de atividades do console e do banco de dados núcleo.

Esta caixa de diálogo contém as seguintes opções:

- **Selecione um tipo de atividade:** Especifique que informações de atividade de componente de segurança você quer depurar.
- **Selecionar computadores:** Especifique quais atividades de segurança dos dispositivos gerenciados foram limpas. (Nota: Você precisa ser um administrador para executar esta tarefa.)
- **Selecionar intervalo de datas:** Especifique a data mais cedo possível a partir da qual a atividade de segurança é purgada. Ou, exclua todas as informações existentes usando a opção **Todos os registros**.
- **Limpar:** Remove completamente os registros de atividade dos componentes de segurança que você selecionar.

Configurar configurações do alerta de segurança

Você pode configurar alertas relacionados a segurança de forma a ser notificado quando eventos específicos forem detectados em dispositivos gerenciados no seu sistema. O Antivirus de segurança usa a ferramenta padrão de alerta da LANDesk.

O diálogo de configurações de alerta contém opções para ambos os alertas, de vulnerabilidade e antivírus.

Alertas de antivírus

As definições de alerta de antivírus são encontradas na guia **Antivirus** da caixa de diálogo **Configurações de alerta**.

É necessário primeiro configurar os alertas de antivírus na ferramenta Configurações de alerta no console. Os alertas de antivírus incluem:

- Falha em uma ação de alerta do antivírus
- Êxito em uma ação de alerta do antivírus
- Alerta de ataques de vírus (por vírus)

Os seguintes eventos de antivírus podem gerar alertas de antivírus:

- A remoção do vírus falhou
- A remoção do vírus teve êxito
- A quarentena falhou
- A quarentena teve êxito
- A exclusão falhou
- A exclusão teve êxito

Selecione os alertas que desejar gerar. A opção intervalo de tempo permite que você impeça a ocorrência de alertas em demasia. Se houver mais de um alerta (para qualquer disparo de antivírus) durante um intervalo especificado, ele será ignorado.

Você pode ver o histórico completo de alerta de antivírus de um dispositivo na caixa de diálogo Informações de segurança e patch. Clique com botão direito em um dispositivo, selecione **Informações de segurança e patch**, selecione o tipo de Antivírus na lista **Tipo** e, em seguida, selecione o objeto Histórico de antivírus.

Alertas de vulnerabilidade

Para obter informações sobre alertas de vulnerabilidade, consulte "Configurar alertas de patch e conformidade" na página 615.

Segurança de ponto final

Visão geral da Segurança de terminais

A nova ferramenta de Segurança de terminais é, na verdade, um conjunto de recursos complementares e cenários que permite que você configure e implemente uma segurança de sistema forte para os dispositivos administrados na rede. Você pode limitar as conexões de rede para dispositivos administrados, o acesso à essas máquinas por outros tipos de dispositivos e usar o Host Intrusion Prevention System (HIPS) e as ferramentas do LANDesk Firewall para prevenir a execução não autorizada de operações.

O Endpoint security fornece uma defesa impenetrável para todos os dispositivos protegidos dentro da rede LANDesk e o perímetro da rede, assim como usuários de dispositivos móveis; fornecendo um total controle sobre o acesso para e a partir desses dispositivos e, também, as ações permitidas neles.

Embora o Endpoint Security seja um agente único consolidado que é distribuído para dispositivos alvo, ele é totalmente configurável e fornece serviços para vários componentes de segurança.

Componentes do Endpoint Security

Os componentes do Endpoint Security são:

- **Alerta ao local:** Fornece controle de conexão de rede com Alerta ao local e recursos de confiáveis de localização. Para obter mais informações, consulte, see "Ajuda da Segurança de terminais" na página 678.
- **Host Intrusion Prevention System (HIPS)** Previne intrusões proibidas. Para obter mais informações, consulte "Visão geral do Host Intrusion Prevention System (HIPS)" na página 681.
- **LANDesk Firewall** Previne operações proibidas de aplicação e conexões. Para obter mais informações, consulte "Configurar parâmetros de firewall LANDesk" na página 695.)
- **Controle de dispositivo** Restringe acesso para volumes de armazenamento, dispositivos, interfaces, e assim por diante. Para saber mais, consulte "Controle de dispositivo" na página 700.
- **Lista de arquivos confiáveis:** Listas são compostas de arquivos configurados com um conjunto de direitos específicos (privilégios ou autorizações) que permitem ou negam certas ações de serem realizadas naquele arquivo *por*um aplicativo

Com o Endpoint Security você pode definir locais confiáveis (conexões de rede) para dispositivos gerenciados, criar configurações para cada um dos componentes do Endpoint Security acima relacionados e distribuir essas configurações com base no fato de o dispositivo estar conectado a um local confiável da rede ou a um local exeterno confiável.

Conforme declarado acima, o Endpoint Security é um agente único que aplica as regras de proteção nos dispositivos gerenciados e controla a funcionalidade de cada um dos componentes de segurança. O Endpoint Security tem a flexibilidade de permitir que você habilite e configure os componentes de segurança independentemente ou por uma distribuição combinada. Por exemplo, você pode distribuir a proteção HIPS somente ou a HIPS e o Controle de dispositivos (através de suas configurações respectivas) ou qualquer outroa combinação de componentes de segurança.

Esta seção descreve como habilitar o Endpoint Security nos dispositivos gerenciados e direciona você para as informações sobre cada um dos componentes de Endpoint Security abrangidos.

Habilitar e distribuir o Endpoint Security

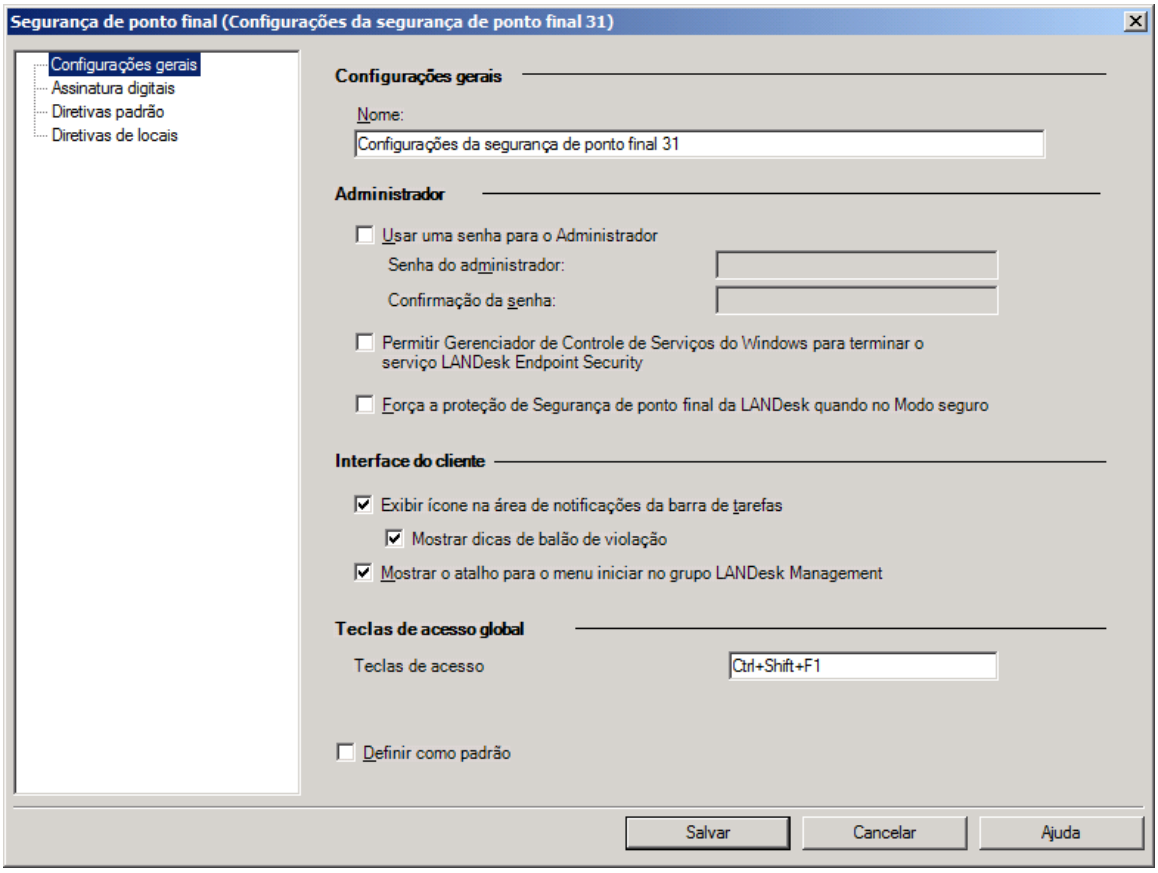
O Endpoint Security é habiltado nos dispositivos gerenciados através da distribuição e personalização das configurações do Endpoint Security.

O Endpoint Security pode ser habilitado em dispositivos gerenciados através da configuração de agente inicial. Também é possível usar uma tarefa de de alteração de configurações para instalar ou atualizar as configurações do Endpoint Security nos dispositivo gerenciado.

Criação de configurações para o Endpoint Security

Para criar configurações do Endpoint Security

1. Na janela da ferramenta **Configurações de agente**, clique com o botão direito em **Segurança de terminal** e em **Novo**.


Segurança de ponto final (Configurações da segurança de ponto final 31)
Configurações gerais
Assinatura digitais
Diretivas padrão
Diretivas de locais
Configurações gerais
Nome:
Configurações da segurança de ponto final 31
Administrador
Usar uma senha para o Administrador
Senha do administrador:
Confirmação da senha:
Permitir Gerenciador de Controle de Serviços do Windows para terminar o serviço LANDesk Endpoint Security
Força a proteção de Segurança de ponto final da LANDesk quando no Modo seguro
Interface do cliente
Exibir ícone na área de notificações da barra de tarefas
Mostrar dicas de balão de violação
Mostrar o atalho para o menu iniciar no grupo LANDesk Management
Teclas de acesso global
Teclas de acesso
Ctrl+Shift+F1
Definir como padrão
Salvar
Cancelar
Ajuda

2. Na página **Configurações gerais**, digite um nome para as configurações do HIPS e, em seguida, especifique os requisitos gerais e as ações. Clique em **Ajuda** para encontrar mais informações sobre uma opção.

3. Se quiser gerenciar conexões de rede, selecione a opção **Usar alerta ao local**. Quando esta opção é selecionada, a página **Local confiável** é exibida. Além disso, ao selecionar esta opção, são disponibilizados dois grupos separados na página **Diretivas de segurança**, um para quando o dispositivo está dentro do local confiável e um para quando o dispositivo está fora do do local confiável. Se o alerta ao local não estiver habilitado, só um grupo de diretiva é necessário.
4. Na página **Diretivas de segurança**, selecione quais componentes do Endpoint Security você quer distribuir para os dispositivos alvo com estas configurações de Endpoint Security.
5. Na página **Local confiável**, defina as conexões de rede permitidas (por endereço IP, faixa de IP ou sub-rede).
6. Clique em **Salvar**.

Uma vez configuradas, você poderá distribuir as configurações para dispositivos alvo com uma tarefa de instalação ou de atualização ou uma tarefa de mudança de configurações.

O que acontece em um dispositivo com o Endpoint Security

Esta seção descreve como o cliente do Endpoint Security aparece nos dispositivos gerenciados em que ele está instalado, o que acontece nos dispositivos de usuários finais quando protegidos pelo Endpoint Security e as ações que os usuários finais podem executar quando uma violação de segurança for descoberta.

Interface do usuário do cliente

Quando o Endpoint Security for distribuído para os dispositivos gerenciados, seu cliente poderá ser acessado através do menu Iniciar ou do ícone da bandeja do sistema.

IMPORTANTE: Proteção da senha do administrador
Se o administrador ativou a opção de proteção por senha nas configurações do Endpoint Security, a senha correta deverá ser digitada para que seja possível acessar e usar os recursos do cliente.

Ícone da bandeja do sistema

O ícone da bandeja do sistema mostra se o componente HIPS do Endpoint Security está sendo executado no modo de aprendizagem ou de bloqueio automático.

Os usuários finais podem clicar com o botão direito do mouse no ícone para acessar seu menu de atalho e selecionar as seguintes opções:

- **Abrir:** abre o cliente.
- **Opções:** exibe as opções que foram configuradas pelo administrador no console (somente leitura).
- **Modo automático:** permite que o componente HIPS execute no modo automático, no qual todas as violações de segurança predefinidas são bloqueadas.
- **Modo de aprendizagem:** permite que o componente HIPS execute no modo de aprendizagem, no qual todas as violações de segurança são permitidas, mas também são monitoradas e gravadas em um arquivo de histórico de ações.
- **Instalar software:** abre uma janela do Explorer que permite que o usuário final selecione um programa de instalação para executar.
- **Descarregar:** permite que o usuário final desinstale o cliente do próprio computador.

Ações do usuário final

O cliente é exibido numa janela que inclui os seguintes elementos, onde o usuário final pode:

- Exibir o log de atividade.
- Exibir as opções que foram configuradas pelo administrador no console (somente leitura).
- Na página **Status**: Exibir informações do componente HIPS, o modo de operação atual e as atividades em andamento no cliente. Mude o modo de operação (senha de autorização talvez seja exigida).
- Na página **Programas**: Exibir os aplicativos em execução e suas autorizações. Selecionar os programas e exibir todas as suas autorizações ou eliminar o processo. Modificar as opções de exibição.
- Na página **Inicialização**: Exibir e editar o conteúdo da inicialização do sistema. Além disso, de serviços em execução no cliente e extensões do Internet Explorer.
- Na página **Proteção**: Exibir os direitos de acesso dos programas e as proteções de pastas. Criar, editar e excluir regras de proteção de arquivos. Alterar a prioridade das regras na lista ordenada.
- Na página **Certificação**: Exibir programas com certificações de arquivos especiais. Adicionar e excluir certificações de arquivos.

Ajuda da Segurança de terminais

Use este diálogo para criar e editar configurações do Segurança de terminais.

Esta caixa de diálogo contém as seguintes páginas:

- "Sobre a página Segurança de terminais: Página de configurações gerais" na página 678
- "Ajuda da Segurança de terminais" na página 678
- "Na página Segurança de terminais: Diretivas padrão" na página 679
- "Na página Segurança de terminais: Página de diretivas do local" na página 680

Sobre a página Segurança de terminais: Página de configurações gerais

Use esta página para configurar o alerta ao local (rede confiável) e outras configurações de acesso.

- **Nome:** Identifica as configurações com um nome exclusivo.
- **Usar o alerta ao local:** Permite gerenciar conexões de rede. Você pode restringir endereços IP de rede aos quais os dispositivos são permitidos conectar. As restrições de rede são configuradas especificando-se que endereços de rede são permitidos. O dispositivo pode receber somente endereços IP dentro do intervalo de endereços explicitamente permitidos.
- **Permite ao Gerenciador do controle de serviço do Windows pare o serviço do Segurança de terminais:** Permite que o usuário final interrompa o serviço de Segurança de terminais no cliente.
- **Senha do administrador:** Especifica a senha exigida nos dispositivos configurados com estas configurações de Segurança de terminais para executar determinadas ações no dispositivo protegido. Ações que exigem uma senha incluem: acessar a interface do cliente HIPS, instalar software não assinado, autorizar violações do HIPS, descarregar o HIPS, apagar o relatório local e alternar o modo de operação do HIPS.

- **Opções de interface de usuário do cliente:** Especifica como o cliente Segurança de terminais cliente exibe os dispositivos gerenciados.
  - **Exibe o ícone da área de notificação:** Exibe o ícone da área de notificação na interface do cliente.
  - **Mostra mensagens pop-up de violação:** Mostra uma mensagem no dispositivo do usuário final se ocorrer uma operação de bloqueio.
  - **Exibe o atalho do menu Iniciar no grupo do LANDesk Management:** Exibe um ícone do programa para o cliente de Segurança de terminal no menu Iniciar (clique em **Iniciar > Programas > LANDesk Management**)
- **Atalhos globais:** Especifica os atalhos usados para recursos específicos da Segurança de terminais.
  - **Controle de dispositivos por teclas de atalho:** Permite que você defina uma sequência de teclas de atalho que permite que os administradores do sistema tenham acesso temporário a um dispositivo bloqueado. Você pode modificar o atalho padrão, que é Ctrl+Shift+Up. Para entrar a sequência desejada de atalho, coloque o cursor na caixa de texto, e então pressione (e mantenha) as chaves na ordem que você quer.
- **Definir como padrão:** Atribui estas configurações como configurações padrão das tarefas que usam configurações de Segurança de terminais.
- **Salvar:** Salva as alterações e fecha a caixa de diálogo.

Na página Segurança de terminais: Página de assinaturas digitais

Use esta página para exibir e gerenciar certificações de arquivos. Listas de arquivos confiáveis são compostas de arquivos com um conjunto de permissões específicas (privilégios ou autorizações) que permitem e negam determinadas ações que podem ser executadas naquele arquivo *por* um aplicativo.

Esta página contém as seguintes opções:

- **Listas de arquivos confiáveis:** Exibe a lista de arquivos com permissões configuradas para HIPS.
  - **Adicionar:** Abre a caixa de diálogo Configurar a lista de arquivos confiáveis, a partir de onde você pode gerenciar as listas de arquivos confiáveis.
  - **Editar:** Permite editar a lista de arquivos confiáveis selecionada.
  - **Remover:** Exclui a lista de arquivos confiáveis selecionada.
- **Opções de atividades de aprendizado:** Especifica como a atividade dos arquivos é manuseada quando o modo de proteção é definido como aprendizado.
  - **Lista de aprendizado:** Exibe a lista de arquivos confiáveis para o qual a atividade de arquivo de aprendizado é aplicada.
  - **Adicionar atividade de aprendizado somente na lista de aprendizado:** Limita a atividade do arquivo de aprendizado a ser aplicado somente a lista de arquivos especificados.
  - **Adicionar atividade de aprendizado em cada lista onde o mesmo arquivo já existe:** Permite que a atividade de arquivo de aprendizado seja aplicada a qualquer lista de aquivos que contenha aquele arquivo.

Na página Segurança de terminais: Diretivas padrão

Use esta página para configurar diretivas de segurança para dispositivos dentro da rede confiável e diretivas para dispositivos fora da rede confiável.

- **Se estiver dentro do local confiável:** Especifique as configurações de componente a serem aplicadas aos dispositivos quando eles são conectados a um local confiável.

- **Se estiver fora do local confiável:** Especifica as configurações de componente a serem aplicadas aos dispositivos quando eles não estão conectados a um local confiável.

Na página Segurança de terminais: Página de diretivas do local

Use esta página para definir os locais confiáveis. Um local confiável é composto de uma coleção de endereços de rede, por endereço de IP, faixa de IP ou sub-rede.

Essa página contém as seguintes opções:

- **Use reconhecimento de local (diretivas de instalação para múltiplos locais)**
  - **Adicionar:** Clique para adicionar uma nova diretiva de conhecimento de local confiável.
  - **Editar:** Permite modificar o local confiável existente.
  - **Remover:** Remove os locais confiáveis selecionados.

NOTA: Diretiva padrão
A diretiva padrão será aplicada quando um dispositivo não está associado com nenhum dos locais relacionados.

Sobre a caixa de diálogo Adicionar local

Use esta caixa de diálogo para criar um novo local para suas diretivas de conhecimento de local confiável. Você pode inserir um Endereço IP, um intervalo de IP ou um endereço de sub-rede

Esta caixa de diálogo contém as seguintes opções:

- **Nome:**
- **Condições:**
  - **Tipo:**
  - **Valor:**
  - **Adicionar:**
  - **Editar:**
  - **Excluir:**
  - **Importar:**
- **Servidor núcleo:**
  - **Verificação da existência do servidor núcleo na rede:** Selcione esta opção para se assegurar de que o servidor núcleo está em execução na rede antes que um dispositivo tenha a permissão de conectar àquela rede. Às vezes, uma faixa de endereços IP pode ser usada por mais de uma rede e essa opção fornece segurança adicional ao restringir o acesso à rede. Se nenhum servidor núcleo for encontrado na rede sendo acessada, a conexão será desativada. (Nota: Deixe esta opção em branco se tiver certeza que os endereços de rede na lista de acesso são confiáveis ou se preferir reduzir o tráfego na rede, deixando de enviar pings ao servidor núcleo.
  - **Adicionar:** Permite adicionar um servidor núcleo à lista.
  - **Remover:** Remove os servidores núcleo selecionados.
- **OK:**
- **Cancelar:**

Tópicos relacionados

Visão geral do Host Intrusion Prevention System (HIPS)

HIPS significa Host-based Intrusion Prevention System (sistema de prevenção de intrusões baseado em hosts). O HIPS fornece uma camada de proteção extra adicionada sobre o antivírus, anti-spyware, gerenciamento de patches e na configuração de firewall para impedir a execução de atividades mal-intencionadas em seu computador. O HIPS monitora de forma constante e contínua processo, arquivos, aplicativos e chaves do Registro especificados para impedir comportamentos não autorizados. Você controla quais aplicativos podem ser executados nos dispositivos e como são suas permissões de execução.

Como o HIPS é um sistema baseado em regras, e não em definições (isto é, baseado em assinaturas), esse recurso pode ser mais eficiente na proteção de sistema contra ataques dia zero (exploração de código vulnerável antes da descoberta da exposição, definidas e a disponibilização de patches).

Ao contrário da detecção e correção de vulnerabilidades, da detecção e remoção de spyware ou da análise antivírus e quarentena, a proteção do HIPS não necessita atualizações contínuas de arquivos, tais como, arquivos de patch, arquivos de definição/padrões ou de bancos de dados de assinaturas.

O HIPS protege servidores e estações de trabalho ao inserir agentes de software entre os aplicativos e o kernel do sistema operacional. Ao usar regras predeterminadas baseadas no comportamento típico dos ataques de malware, esses sistemas avaliam atividades como solicitações de conexão de rede, tentativas de leitura ou gravação na memória ou tentativas de acessar aplicativos específicos. Comportamentos reconhecidos como apropriados são permitidos, atividades identificadas como inadequadas são bloqueadas e qualquer outro comportamento suspeito é marcado para avaliação adicional.

A ferramenta HIPS e os recursos são acessados do console principal (**Ferramentas > Segurança e Conformidade > Configurações de agente**). A ferramenta HIPS permite criar tarefas de instalação, atualização e remoção do agente HIPS, configurar opções do HIPS que podem ser distribuídas para os dispositivos alvo que você deseja proteger e personalizar as opções de exibição/interação do HIPS que determinam a aparência e o modo de operação do HIPS nos dispositivos gerenciados, além de quais opções interativas estão disponíveis para os usuários finais. Você também pode exibir a atividade do HIPS e as informações de status para os dispositivos protegidos.

Componente de segurança de ponto final

HIPS é um dos componentes da solução abrangentes Segurança de ponto final juntamente com o Alerta ao local (controle de conexão de rede), a LANDesk Firewall e as ferramentas de Controle de dispositivo.

Segurança preventiva

O HIPS protege preventivamente os seus dispositivos ao:

- Fornecer proteção em nível de kernel contra aplicativos que poderiam tentar modificar os binários (ou quaisquer arquivos especificados) em seu computador ou na memória de aplicativos dos processos em execução. Bloqueio de alterações em determinadas áreas do Registro e capacidade de detectar processos de kits de usuário raiz.
- Usar proteção de memória contra estouros de buffer e explorações do heap.

- Executar esquemas de proteção para impedir que um agressor compile e execute código em um segmento de dados.
- Monitorar acessos não autorizados ou fora do normal a arquivos.
- Oferecer proteção em tempo real para o seu computador sem depender de bancos de dados de assinaturas.

Segurança de nível do sistema

O HIPS oferece a seguinte proteção em nível de sistema:

- Proteção de sistema de arquivos em nível de kernel baseada em regras
- Proteção do Registro
- Controle de inicialização
- Detecção de kits de usuário raiz disfarçados
- Filtragem de rede
- Certificação de processos e arquivos/aplicativos
- As regras de proteção de arquivo que restringem as ações que programas executáveis podem executar em arquivos especificados

Recursos do console do HIPS

O HIPS oferece aos administradores a capacidade de definir e gerenciar perfis separados para diferentes grupos de usuários com configurações de HIPS. As configurações do HIPS comportam as necessidades de todos os grupos de usuários ao permitir que os administradores criem várias configurações altamente flexíveis para os diferentes perfis de usuário.

A configuração do HIPS pode incluir proteção de senha personalizada, manuseio do WinTrust, modo de proteção, listas de permissão personalizadas, diretrizes de controle de acesso de aplicativo e de rede, certificações de arquivos e regras de proteção a arquivos.

Recursos do cliente do HIPS

O cliente do HIPS (distribuídos a dispositivos gerenciados) oferece aos administradores uma nova ferramenta avançada para controlar quais aplicativos são executados em desktops e servidores e a permissão de execução a eles concedida.

O software do cliente do HIPS usa técnicas comprovadas de heurística e reconhecimento de comportamento para identificar ações e padrões típicos de código mal-intencionado. Por exemplo, um arquivo que tentar gravar no Registro dos sistema poderia ser bloqueado e marcado como potencialmente mal-intencionado. O cliente do HIPS usa várias técnicas proprietárias para detectar o malware de forma confiável, até mesmo antes da identificação de uma assinatura.

Plataformas de dispositivo com suporte

Para obter informações detalhadas atualizadas sobre quais plataformas de cliente são compatíveis HIPS, consulte o documento 'OS Compatibility Feature Matrix' na comunidade de usuários da LANDesk:

Página inicial da Comunidade de usuários da LANDesk

IMPORTANTE: Não há suporte ao HIPS em servidores núcleo ou em núcleos de rollup
Você não deve instalar/distribuir o HIPS em um servidor núcleo ou núcleo de rolllup. No entanto, é

possível distribuir o HIPS para um console adicional.

Produtos de antivírus suportados

HIPS é compatível com a solução LANDesk Security Suite Antivirus e com vários produtos antivírus de terceiros. Compatibilidade significa que o HIPS não interfere com os processos de antivírus como análises, proteção em tempo real, etc.

Verifique se os dispositivos gerenciados que deseja configurar com o HIPS tem um dos seguintes produtos antivírus instalado:

- LANDesk Antivirus
- Symantec* Antivirus (versões 7, 8, 9, 10.1, 10.2)
- McAfee VirusScan (versões 7.0, 8.0, 8.5i)
- Trend Micro PC-cillin (versões 2005, 2006)
- Trend Micro OfficeScan (versões 6.5, 7.3)
- Trend Micro ServerProtect (versão 5.58)
- CA eTrust InoculateIT (versão 6.0)
- CA eTrust Antivirus (versões 7.0, 7.1, 8.0, 8.1)
- ESET NOD32 (versão 2.7)

NÃO distribua o HIPS para dispositivos com qualquer outro produto antivírus instalado.

Licenciamento do HIPS

Para acessar a ferramenta HIPS, você deve ativar primeiro seu servidor núcleo com uma licença do HIPS.

Para encontrar mais informações sobre o licenciamento do HIPS contate o revendedor ou visite o site do LANDesk:

LANDesk Home Page

Administração com base em funções com HIPS

O HIPS, como o Patch e Conformidade, utiliza a administração baseada em funções para permitir o acesso dos usuários aos recursos. A administração com base em funções é a estrutura de acesso e segurança que permite aos administradores LANDesk restringir o acesso a ferramentas e dispositivos. Cada usuário recebe funções e escopo específicos que determinam quais recursos podem usar e quais dispositivos podem gerenciar.

Os Administradores atribuem essas funções a outros usuários com a ferramenta Gerenciar usuários no console. HIPS é incluso no direito Configurações de agente que aparece sob o grupo de direitos de segurança no diálogo Funções. Para ver e usar os recursos do HIPS, os direitos necessários de Configurações de agente precisa ser atribuído ao usuário.

IMPORTANTE: Permissões de grupos LANDesk Script Writers são necessárias
Para criar tarefas agendadas e diretivas na ferramenta Patch e conformidade e a ferramenta Configurações de segurança (para tarefas de análise de segurança e conformidade, tarefas de reparo e tarefas de mudanças de configurações), um usuário precisa ter permissão de grupo LANDesk Script

Writers. Em outras palavras, eles precisam pertencer a um grupo que tenha permissão de LANDesk Script Writers atribuída. Para obter mais informações sobre a administração baseada em funções, consulte "Gerenciamento de usuários" na página 38.

Com o direito Configurações de agente, você pode fornecer aos usuários a habilidade de:

- Ver e acessar os recursos do Host Intrusion Prevention System (HIPS) no menu Ferramentas do console e na Caixa de ferramentas
- Configurem dispositivos gerenciados para a proteção do HIPS
- Gerenciem as configurações do HIPS (proteção de senha, tratamento de código assinado, modo de proteção, certificações de arquivos, regras de proteção de arquivos, etc.)
- Distribuam tarefas de instalação ou atualização do HIPS e tarefas de alteração de configurações
- Exibam a atividade do HIPS para dispositivos protegidos
- Configurar definições de limites de dados do HIPS para a gravação e a exibição de atividade do HIPS

Descrição das principais tarefas do HIPS

A lista abaixo descreve as principais tarefas envolvidas na configuração, implementação e uso da proteção HIPS. Consulte os tópicos de ajuda específicos do recurso para obter informações conceituais e práticas detalhadas.

- Configuração de dispositivos gerenciados para proteção do HIPS (distribuição do agente para os dispositivos alvos).
- Configuração das opções do HIPS com definições HIPS como o tratamento de código atribuído, modo de proteção, listas de permissão (aplicativos com permissão para executar em dispositivos), certificações de arquivos, regras de proteção de arquivos e opções de interatividade de usuário final.
- Descoberta do comportamento de arquivos e aplicativos nos dispositivos com o modo de aprendizagem do HIPS.
- Imposição da proteção do HIPS nos dispositivos gerenciados com o modo de bloqueio automático do HIPS.
- Visualizar atividade do HIPS para dispositivos protegidos

Configurar de dispositivos com a proteção do HIPS

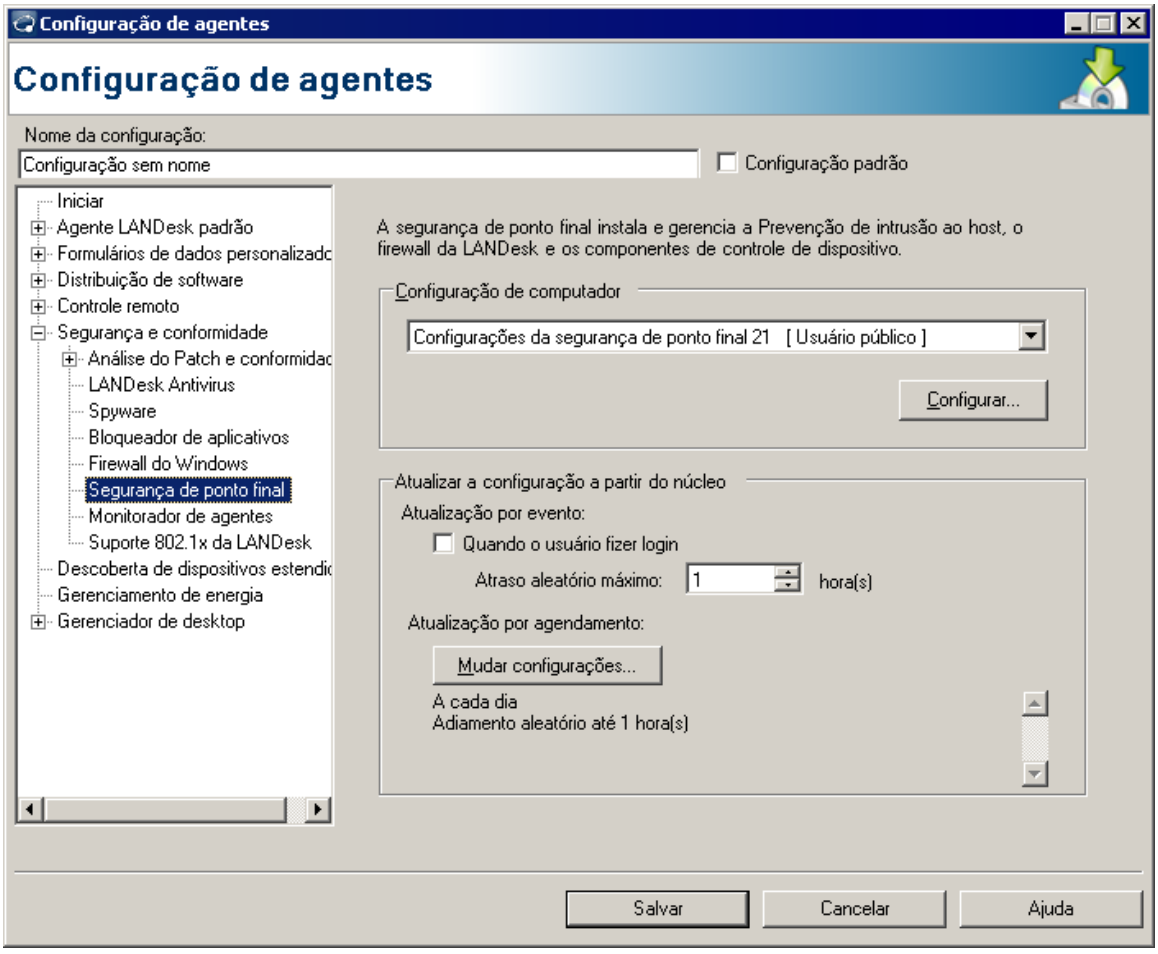
Para que os dispositivos gerenciados possam ser protegidos contra ataques zero-day, eles deverão ter o agente de Segurança de ponto final instalado. O agente de Segurança de ponto final é um serviço único de agente que gerencia todos os componentes de Segurança de ponto final, inclusive o HIPS.

Você pode configurar dispositivos para o HIPS durante a configuração inicial do agente do dispositivo ou com uma tarefa de instalação ou atualização separada.

Para instalar ou atualizar o HIPS em dispositivos gerenciados através da configuração de agente

1. No console, clique em **Ferramentas > Configuração > Configuração de agentes**.
2. Clique no botão da barra de ferramentas **Novas janelas**.
3. Após especificar as configurações desejadas para a configuração do agente, é necessário primeiro clicar na página **Iniciar** e selecionar a opção **Segurança de ponto final** em **Segurança**. (Isso distribui o agente ao dispositivos alvo, mas você ainda precisa selecionar as configuração do HIPS.)

4. Agora, você pode acessar as opções na página **Segurança de ponto final**.

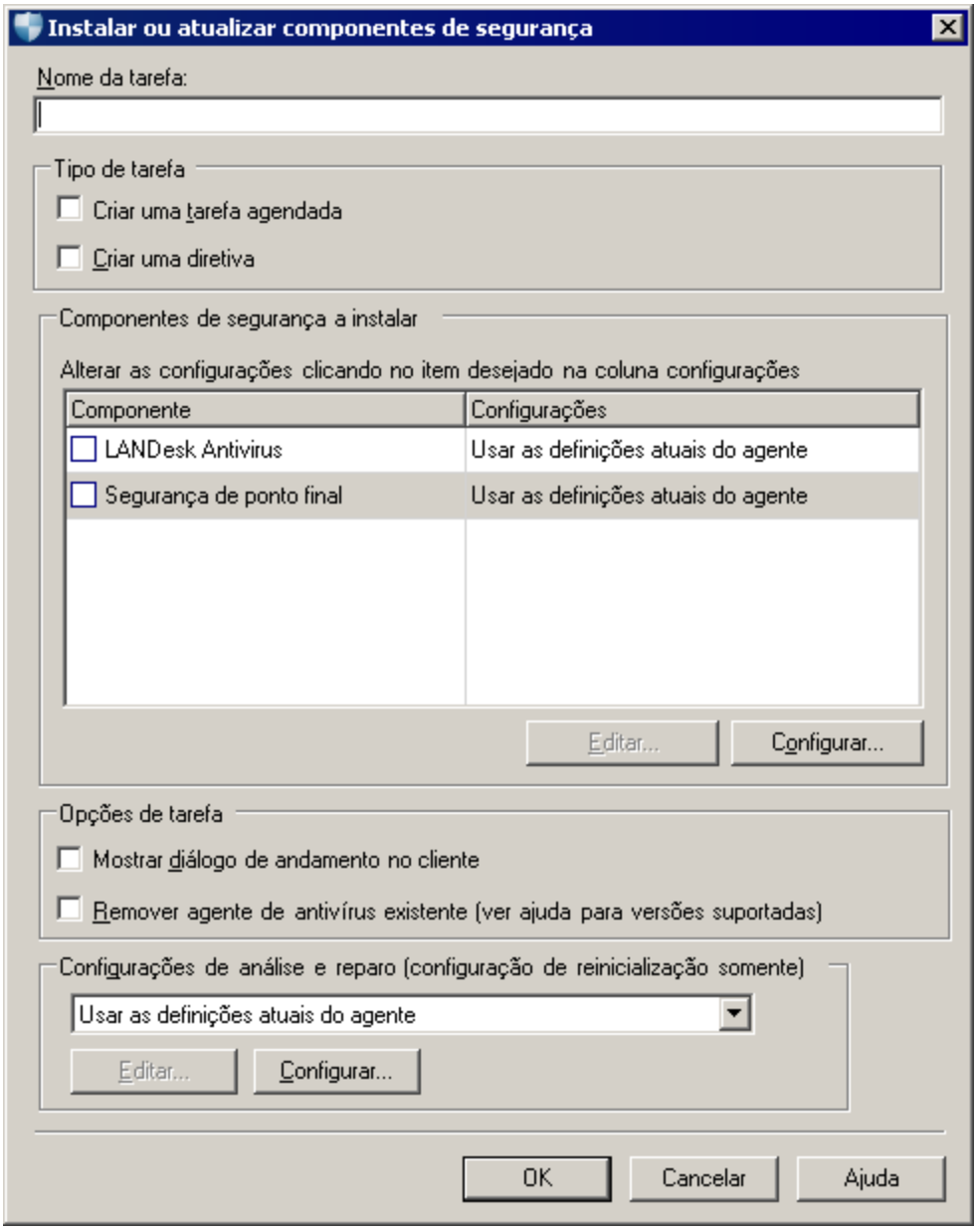


5. Selecione uma das configurações da lista disponível para aplicá-la à configuração do agente que está criando. Você pode criar novas configurações ou editar as configurações existentes clicando em **Configurar**. As configurações de Segurança de ponto final contém configurações HIPS (entre outras configurações de componente de segurança). As configurações do HIPS determinam as opções a seguir: se o cliente do HIPS está protegido por senha, o tratamento do código atribuído do WinTrust, ação em programas adicionados à inicialização do sistema, proteção contra estouros de buffer, modo de operação, listas de permissão, certificações de arquivos e regras de proteção de arquivos.
6. Termine de especificar as definições para a configuração do agente e clique em **Salvar**.

Se desejar instalar ou atualizar o HIPS outra hora, você poderá fazê-lo como uma tarefa separada da ferramenta **Configurações de agente** no console.

Para instalar ou atualizar o HIPS como tarefa separada

1. No console, clique em **Ferramentas > Segurança e Conformidade > Configurações de agente**.
2. Clique no botão **Criar uma tarefa** da barra de ferramentas e clique em **Instalar ou atualizar os componentes de segurança**.



3. Digite um nome para a tarefa.
4. Especifique se a instalação é uma tarefa agendada, baseada em diretivas ou ambas.

5. Selecione as configurações de Segurança de ponto final na lista disponível para aplicá-las à configuração do agente sendo criado. Você pode criar novas configurações ou editar as configurações existentes clicando em **Configurar**. As configurações de Segurança de ponto final contém configurações HIPS (entre outras configurações de componente de segurança).
6. Para mostrar o andamento da instalação na caixa de diálogo do analisador de segurança nos dispositivos alvo, selecione a opção **Mostrar diálogo de andamento no cliente**.
7. Selecione uma configuração de análise e reparo na lista para aplicar sua configuração de reinicialização (somente) à configuração de agente que está criando. Você pode criar novas configurações ou editar as configurações existentes clicando em **Configurar**. Tenha em mente que SOMENTE as opções de reinicialização especificadas nas configurações de análise e reparo que você selecionou são usadas na distribuição do agente de Segurança de ponto final para dispositivos alvo desta configuração de agente. É possível usar uma configuração de análise e reparo que já inclua a configuração de reinicialização desejada ou criar uma nova configuração específica para o seu agente de distribuição.
8. Clique em **OK**.

Remover do HIPS dos dispositivos

Se desejar remover o HIPS dos dispositivos gerenciados, você também poderá fazê-lo como uma tarefa do console.

Para remover o HIPS

1. No console, clique em **Ferramentas > Segurança e Conformidade > Configurações de agente**.
2. Clique no botão **Criar uma tarefa** da barra de ferramentas e clique em **Remover componentes de segurança**.
3. Digite um nome para a tarefa.
4. Especifique se a instalação é uma tarefa agendada, baseada em diretivas ou ambas.
5. Selecione o componente de Segurança de ponto final para remover este agente que inclui HIPS.
6. Para mostrar o andamento da instalação na caixa de diálogo do analisador de segurança nos dispositivos alvo, selecione a opção **Mostrar diálogo de andamento no cliente**.
7. Selecione uma configuração de análise e reparo na lista disponível para aplicar sua configuração de reinicialização à tarefa que está criando. Você pode criar novas configurações ou editar as configurações existentes clicando em **Configurar**. A tarefa usará as opções de reinicialização das configurações de análise e reparo SOMENTE, o que determina os requisitos de reinicialização e as ações nos dispositivos alvo durante a remoção do agente.
8. Clique em **OK**.

Personalizar da proteção HIPS com configurações HIPS

As configurações do HIPS lhe dá o controle total sobre como o produto opera nos dispositivos alvo e sobre quais opções estão disponíveis para os usuários finais.

Esta seção descreve o modo como criar e gerenciar configurações HIPS:

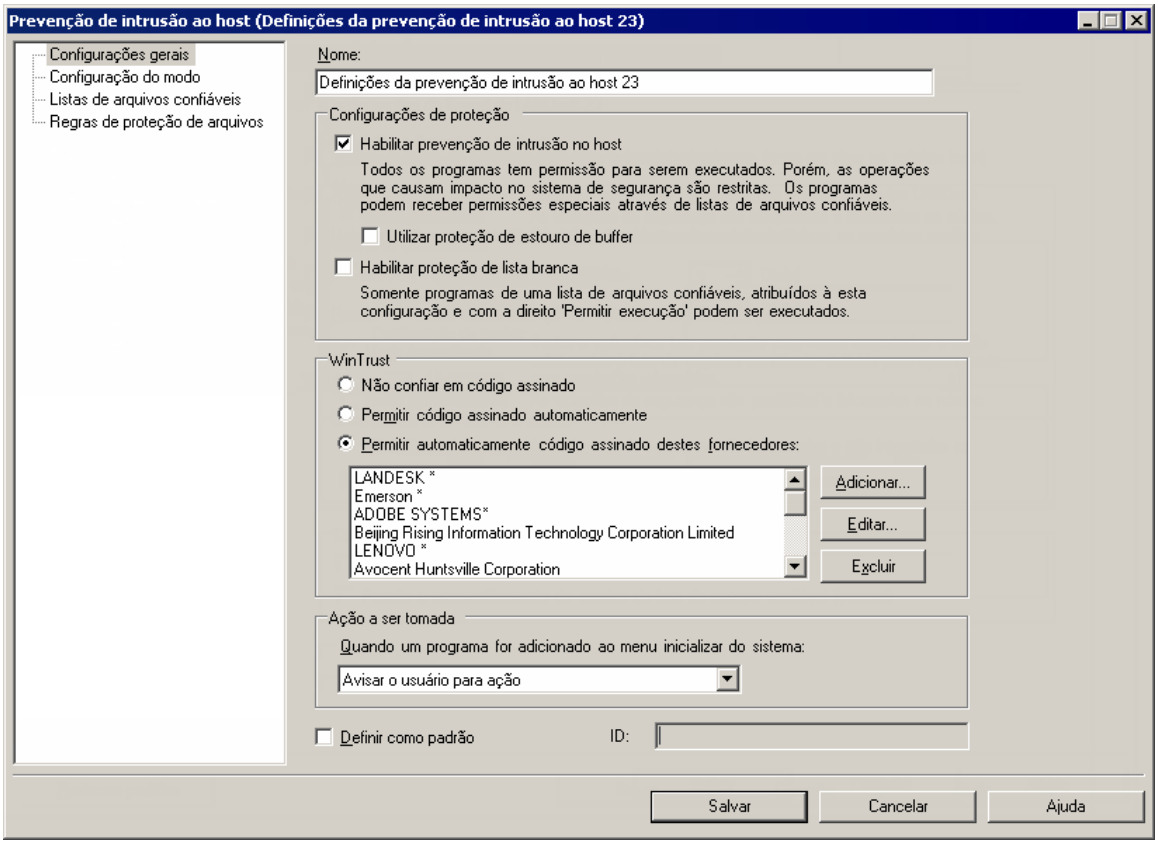
- "Criar configurações do HIPS" na página 688
- "Mudar configurações padrão do HIPS" na página 689
- "Exibir configurações do HIPS de dispositivos no Inventário" na página 689
- "Ajuda do HIPS" na página 690

Criar configurações do HIPS

Você pode criar e aplicar as configurações do HIPS em uma instalação do HIPS, atualizar a tarefa ou mudar as tarefas das configurações. Você pode criar quantas configurações do HIPS desejar. As configurações do HIPS podem ser criadas para um fim, tempo ou conjunto de dispositivos alvo específicos.

Para criar configurações do HIPS

1. Na janela da ferramenta **Configurações de agente**, clique com o botão direito em **Prevenção de intrusão no host** e clique em **Novo**.


Prevenção de intrusão ao host (Definições da prevenção de intrusão ao host 23)
Configurações gerais
Configuração do modo
Listas de arquivos confiáveis
Regras de proteção de arquivos
Nome:
Definições da prevenção de intrusão ao host 23
Configurações de proteção
Habilitar prevenção de intrusão no host
Todos os programas tem permissão para serem executados. Porém, as operações que causam impacto no sistema de segurança são restritas. Os programas podem receber permissões especiais através de listas de arquivos confiáveis.
Utilizar proteção de estouro de buffer
Habilitar proteção de lista branca
Somente programas de uma lista de arquivos confiáveis, atribuídos à esta configuração e com a direito 'Permitir execução' podem ser executados.
WinTrust
Não confiar em código assinado
Permitir código assinado automaticamente
Permitir automaticamente código assinado destes fornecedores:
LANDESK *
Emerson *
ADOBE SYSTEMS*
Beijing Rising Information Technology Corporation Limited
LENOVO *
Avocent Huntsville Corporation
Adicionar...
Editar...
Excluir
Ação a ser tomada
Quando um programa for adicionado ao menu inicializar do sistema:
Avisar o usuário para ação
Definir como padrão
ID:
Salvar
Cancelar
Ajuda

2. Na página **Configurações gerais**, digite um nome para as configurações do HIPS e, em seguida, especifique os requisitos gerais e as ações. Clique em "Ajuda do HIPS" na página 690 para encontrar mais informações sobre uma opção.
3. Na página **Configuração de modo**, selecione se você deseja reforçar o modo de proteção de bloqueio automático ou o modo de aprendizagem do HIPS. Você também pode selecionar criar uma lista de permissão (aplicativos com permissão de executar em dispositivos), com base nos arquivos atualmente certificados e, se desejar, que a lista de permissão funcione inicialmente por um período especificado de tempo e depois reforce o modo de bloqueio automático ou continue a usar o modo de aprendizagem. (**NOTA:** Se você selecionar o modo de aprendizado como modo de proteção geral e quiser gerar uma lista de permissões, a opção de modo automático será desativada.
4. Na página Certificações de arquivos, adicione, modifique ou exclua certificações de arquivos.

5. Na página **Regras de proteção de arquivos**, adicione, modifique, priorize ou exclua regras de proteção de arquivos. O HIPS inclui um conjunto pré-definido (padrão) de regras de proteção.
6. Em qualquer página de configurações do HIPS, clique em **Salvar** a qualquer momento para salvar suas opções de configurações do HIPS ou clique em **Cancelar** para sair da caixa de diálogo sem salvar as configurações.

Uma vez configuradas, você poderá distribuir as configurações do HIPS para dispositivos alvo com uma tarefa de instalação ou de atualização ou uma tarefa de mudança de configurações.

Mudar configurações padrão do HIPS

As configurações do HIPS padrão de um dispositivo são distribuídas como parte da configuração inicial do agente. Em algum momento, no entanto, talvez você deseje alterar essas configurações do HIPS em determinados dispositivos. O HIPS permite fazer isso sem que seja necessário redistribuir uma configuração de agente inteiramente nova e completa.

Para fazer isso, use a tarefa **Mudar configurações** localizada na lista suspensa do botão **Criar uma tarefa**. A caixa de diálogo que é exibida permite digitar um nome exclusivo para a tarefa, especificar se é uma tarefa agendada ou uma diretiva e selecionar configurações do HIPS existentes como padrão ou usar o botão Editar para criar novas configurações do HIPS como padrão para os dispositivos alvo.

Exibir configurações do HIPS de dispositivos no Inventário

Você pode descobrir e/ou verificar as configurações do HIPS na tela de Inventário de um dispositivo.

Para fazer isso, clique com o botão direito do mouse no dispositivo selecionado e clique em **Inventário >** Management > Prevenção de intrusão ao host.

Combinar certificações de HIPS

Para combinar certificados HIPS de um conjunto de configurações HIPS com um ou mais dos outras configurações HIPS. Isso permite atualizar e compartilhar as configurações do arquivo certificado de forma rápida e fácil.

Combinar arquivos certificados HIPS

1. Na janela da ferramenta **Configurações de agente**, clique com o botão direito em **Host Intrusion Prevention** e clique em **Combinar arquivos certificados**.
2. Selecione uma configuração de origem na lista suspensa.
3. Selecione se deseja mesclar diferenças nos arquivos certificados ou simplesmente substituir todos os arquivos certificados.
4. Selecione a(s) configuração(ões) alvo.
5. Clique em **OK**.

Ajuda para combinar arquivos certificados HIPS

Sobre o diálogo Mesclar arquivos certificados

Use este diálogo para configurar e executar uma mescla de arquivos certificados HIPS entre um ou mais conjuntos de configurações HIPS.

Esta caixa de diálogo contém as seguintes opções:

- **Configuração de origem:** Especifica as configurações HIPS cujos arquivos certificados você quer mesclar com as configurações alvo selecionadas.
- **Mesclar diferenças nos arquivos certificados:** Substitui os arquivos certificados comuns nas configurações alvo por aquelas encontradas na configuração de origem e adiciona arquivos certificados exclusivos da configuração de origem às configurações alvo.
- **Substitui arquivos certificados:** Força os arquivos certificados na configuração de oreigm a substituir todos os arquivos nas configurações alvo.
- **Configurações alvo:** Especifica as configurações alvo que você deseja mesclar com a configuração de origem. Selecione alvos da lista de configurações disponíveis.

Entenda o modo de aprendizagem do HIPS

O HIPS pode ser executado em um dos seguintes modos de proteção: Automático, Aprendizado, Somente log ou Bloqueio.

Uso do modo de aprendizagem do HIPS

A seguir é apresentada uma descrição do processo do modo de aprendizagem do HIPS:

- No modo de aprendizagem, o HIPS identifica que tipos de aplicativos estão instalados no dispositivo, como eles se comportam e seus direitos (privilégios).
- O HIPS monitora a atividade no dispositivo e registra as informações em um arquivo de histórico de ações.
- Os dados de histórico de ações são enviados do dispositivo para o servidor núcleo.
- Os administradores veem o histórico de ações para ver quais aplicativos estão fazendo o que no dispositivo. (Os arquivos/aplicativos e permissões associadas listadas no arquivo histórico de ações (XML) são exibidas na página Certificações de arquivo da caixa de diálogo de configurações HIPS.)
- Os administradores podem personalizar as configurações do HIPS para conceder ou negar privilégios para aplicativos relevantes.

O modo de aprendizagem pode ser aplicado em dispositivos gerenciados, geralmente permitindo que ocorram violações do HIPS até que novas configurações do HIPS sejam distribuídas ou o modo de aprendizagem pode ser aplicado inicialmente por um período especificado de tempo para descobrir quais aplicativos são executados e seus comportamentos, criando uma lista de permissão (aplicativos com permissão para executar nos dispositivos). Se o modo de proteção geral estiver no bloqueio automático, você ainda pode usar o modo de aprendizagem para descobrir os comportamentos dos aplicativos e depois reforçar o modo de bloqueio automático, depois que o período de aprendizagem terminar.

IMPORTANTE: Tanto o servidor núcleo como o dispositivo gerenciado deverão estar operando no modo de aprendizagem para que a comunicação do histórico de atividade ocorra.

Ajuda do HIPS

Use esta caixa de diálogo para criar e editar uma configuração do HIPS (arquivo de configuração). Ao criar configurações do HIPS, você deve definir primeiro os requisitos gerais e as ações e, em seguida, adicionar certificações de arquivos específicas. Você pode criar quantas configurações do HIPS desejar e editá-las a qualquer momento.

Se desejar modificar as configurações padrão do HIPS em um dispositivo sem reinstalar o agente do LANDesk HIPS nem redistribuir uma configuração completa do agente, faça as modificações desejadas em qualquer uma das opções da caixa de diálogo, atribua as novas configurações a uma tarefa de mudança de configurações e distribua essa tarefa para os dispositivos alvo.

Esta caixa de diálogo contém as seguintes opções:

- "Sobre o HIPS: Página de configurações gerais" na página 691
- "Sobre o HIPS: Página Configuração de modo" na página 693
- "Sobre o HIPS: Páginas Regras de proteção de arquivo" na página 694
- "Sobre o HIPS: Diálogo Configurar regra de proteção de arquivos" na página 694

Sobre o HIPS: Página de configurações gerais

Use esta página para configurar as configurações gerais e as ações do HIPS.

Essa página contém as seguintes opções:

- **Nome:** identifica as configurações do HIPS com um nome exclusivo. Este nome é exibido na lista suspensa de configurações do HIPS em um diálogo de tarefa de instalação ou atualização de componentes de segurança.

- **Configurações de proteção:** Há dois tipos de proteção: HIPS e lista branca. Você pode selecionar uma ou ambas. Os dois tipos de proteção usam o mesmo modo de operação o que for selecionado na página de Configuração do modo. (**NOTA:** Há uma exceção esta imposição geral de proteção. Se você especificar o modo Aprender proteção e tiver selecionado a opção de aprendizado SOMENTE lista branca, só serão aprendidos os aplicativos da lista branco e a proteção HIPS é configurada para o modo de bloqueio automático.)
    - **LANDesk Host Intrusion Prevention System:** Ativa a proteção HIPS. Isso permite a todos os programas serem executados (exceto quando a operação do programa ameaça a segurança do sistema) como definidos nas regras de proteção pré-definidas. Você pode conceder permissões especiais à arquivos de programas através de listas de arquivos confiáveis, configurando certificações de arquivos personalizadas. A proteção HIPS observa o comportamento do aplicativo (o aplicativo tem permissão de modificar outro executável, modificar o registro, etc.) e impões as regras de segurança.
        - **Usar a proteção contra estouro de buffer:** Protege os dispositivos da exploração da memória do sistema que tira vantagem de um programa ou processo que está aguardando uma entrada do usuário.Nota:

          NOTA: BOP (Proteção contra estouro de buffer) pode ser ativado nos dispositivos Windows de 32 bits independentemente de o processador ter NX/XD (No eXecute / eXecute Disable) suporte para isso. Se o processador não tiver suporte para NX/XD ele é emulado. Entretanto, se o processador tiver suporte para NX/XD, mas ele estiver desativado no BIOS ou na configuração do BIOS o BOP não pode ser habilitado. Observe que o cliente da Segurança de ponto final mostra se o BOP está habilitado ou desabilitado no dispositivo do usuário final. BOP não é suportado nos dispositivos Windows de 64 bits porque o recurso KPP (Kernel Patch Protection - Proteção de patch do kernel) impede o patch do kernel.IMPORTANTE:

          IMPORTANTE: Recomenda-se enfaticamente testar o BOP (Proteção contra estouro do buffer) nas suas configurações de hardware específicas antes de fazer uma distribuição de ampla escala para dispositivos gerenciados na sua rede. Algumas configurações de processadores mais antigos (antes do Pentium 4 com HT ou HyperThreading) executando determinadas versões SOs Windows podem não suportar completamente a Proteção contra estouro do buffer.

    - **Habilitar a proteção de lista branca:** Ativa a proteção de lista branca. Isto significa que somente aqueles aplicativos presentes na lista de arquivos confiáveis, e aqueles que a certificação do arquivo tem a opção permitir execução ativada, podem ser executados.
        - **Impedir o Windows Explorer de modificar ou excluir arquivos executáveis** Habilite esta opção se você não quer que o Windows serja capaz de modificar ou excluir arquivos executáveis.
- **Ação a executar:** determina a ação tomada quando um programa é adicionado à pasta de inicialização do dispositivo. Esta opção fornece uma segunda linha de defesa para a autorização de processos na pasta de inicialização do sistema. O HIPS monitora o conteúdo da inicialização e se encontrar um novo processo, ele executa a ação que você selecionar (Alertar e perguntar sobre uma ação; Sempre permitir que o programa seja executado; ou Remover o programa da inicialização sem alertar).
- **Definir como padrão:** atribui esta configuração como a configuração padrão das tarefas que usam configurações do HIPS.

- **ID:** identifica esta configuração específica. Esta informação é armazenada no banco de dados e pode ser usada para controlar cada uma das configurações.
- **Salvar:** Salva as alterações e fecha a caixa de diálogo.
- **Cancelar:** Fecha a caixa de diálogo sem salvar as alterações.

Sobre o HIPS: Página Configuração de modo

Use essa página para configurar o modo de operação para proteção do HIPS.

Essa página contém as seguintes opções:

- **Host Intrusion Prevention System** Especifica o comportamento da proteção quando a proteção HIPS é ativada. Quando o modo HIPS está ativado, você pode escolher um dos seguintes métodos operacionais.
  - **Bloqueio:** As violações de segurança são bloqueadas e SÃO gravadas em um arquivo de histórico de ações no servidor núcleo.
  - **Aprendizagem:** Todas as violações de segurança do aplicativo são permitidas, mas o comportamento do aplicativo é observado (ou armazenado) e a informação é enviada de volta ao banco de dados do núcleo em uma lista de arquivos confiáveis. Use esse modo de operação para descobrir o comportamento do aplicativo em um dispositivo ou conjunto de dispositivos específicos e depois use essas informações para personalizar as diretrizes do HIPS antes de distribuir e reforçar a proteção do HIPS por toda a rede.
  - **Apenas log:** As violações de segurança são permitidas e SÃO gravadas em um arquivo de histórico de ações no servidor núcleo.
  - **Silêncio:** As violações de segurança são bloqueadas e NÃO são gravadas em um arquivo de histórico de ações no servidor núcleo.
- **Modo lista branca:** Especifica o comportamento da proteção quando a proteção lista branca é ativada. Proteção de lista branca significa que somente os aplicativos de uma lista de arquivos confiáveis e com a designação de lista branca (aplicativos cuja certificação de arquivo tem a opção de permissão de execução habilitada) têm permissão de serem executados. Quando o modo Whiltelist está ativado, você pode escolher um dos seguintes métodos operacionais.
  - **Bloqueio:** As violações de segurança são bloqueadas e SÃO gravadas em um arquivo de histórico de ações no servidor núcleo.
  - **Aprendizagem:** Todas as violações de segurança do aplicativo são permitidas, mas o comportamento do aplicativo é observado (ou armazenado) e a informação é enviada de volta ao banco de dados do núcleo em uma lista de arquivos confiáveis. Use esse modo de operação para descobrir o comportamento do aplicativo em um dispositivo ou conjunto de dispositivos específicos e depois use essas informações para personalizar as diretrizes do HIPS antes de distribuir e reforçar a proteção do HIPS por toda a rede.
  - **Apenas log:** As violações de segurança são permitidas e SÃO gravadas em um arquivo de histórico de ações no servidor núcleo.
  - **Silêncio:** As violações de segurança são bloqueadas e NÃO são gravadas em um arquivo de histórico de ações no servidor núcleo.

Sobre o HIPS: Páginas Regras de proteção de arquivo

Use esta página para exibir, gerenciar e priorizar regras de proteção de arquivos. As regras de proteção de arquivos são um conjunto de restrições que evita que programas executáveis especificados executem determinadas ações EM arquivos especificados. Com as regras de proteção de arquivos, você pode permitir ou negar acesso, modificação, criação e execução de qualquer programa ou arquivo.

Esta caixa de diálogo contém as seguintes opções:

- **Regras de proteção:** Relaciona todas as regras de proteção de arquivos (padrão) predefinidas fornecidas pela LANDesk, assim como todas as regras de proteção de arquivos que você criou.
  - **Nome da regra:** Identifica a regra de proteção de arquivos.
  - **Restrições:** Exibe ações especfíficas por programas em arquivos que são restritos pela regra de proteção de arquivos.
  - **Programas:** Exibe os programas executáveis protegidos pela regra de proteção.
- **Mover para cima \ para baixo:** Determina a prioridade da regra de proteção de arquivos. Uma regra de proteção de arquivos em posição mais alta na lista tem precedência sobre uma regra em posição mais baixa na lista. Por exemplo, você poderia criar uma regra que restringe o acesso e modificação de um determinado arquivo ou tipo de arquivos por um programa, mas criar outra regra que permite uma exceção àquela restrição por um ou mais programas denominados. Desde que a segunda regra esteja em posição mais alta na lista de regras, ela terá efeito.
- **Redefinir:** Restaura as regras de proteção de arquivo (padrão) predefinidas fornecidas pela LANDesk.
- **Adicionar:** Abre a caixa de diálogo Configurar regra de proteção de arquivos, onde você pode adicionar e remover programas e arquivos, além de especificar restrições.
- **Editar:** Abre a caixa de diálogo Configurar regra de proteção de arquivo, onde você pode editar uma regra de proteção de arquivos existente.
- **Excluir:** Remove a regra de proteção de arquivos do banco de dados.

NOTA: As regras de proteção de arquivos são armazenadas no arquivo FILEWALL.XML, localizado em: ProgramFiles\Landesk\ManagementSuite\ldlogon\AgentBehaviors\Hips_Behavior.ZIP

Sobre o HIPS: Diálogo Configurar regra de proteção de arquivos

Use essa página para configurar as regras de proteção de arquivos.

Esta caixa de diálogo contém as seguintes opções:

- **Nome da regra:** identifica a regra de proteção de arquivo com um nome descritivo.
- **Portas monitoradas**
  - **Todos os programas:** Especifica restringir todos os programas executáveis de executar as ações selecionadas abaixo nos arquivos especificados abaixo.
  - **Programas denominados:** Especifica que somente os programas executáveis da lista têm as restrições selecionadas abaixo aplicadas a eles.
  - **Adicionar:** Permite escolher quais programas são restringidos pela regra de proteção de arquivo. É possível usar nomes de arquivos e caracteres curingas.
  - **Editar:** Permite modificar o nome do programa.
  - **Excluir:** Remove o programa da lista.

- **Exceções**
  - **Permitir exceções para programas certificados:** Permite que qualquer programa executável, que atualmente pertente à lista de arquivos certificados, ignore as restrições associadas a esta regra de proteção de arquivos.
- **Proteger arquivos**
  - **Qualquer arquivo:** Especifica que todos os arquivos são protegidos dos programas especificados acima, de acordo com suas restrições.
  - **Arquivos denominados:** Especifica que somente os arquivos nessa lista são protegidos.
  - **Adicionar:** Permite escolher qual arquivo ou arquivos são protegidos pela regra. É possível usar nomes de arquivos ou caracteres curingas.
  - **Editar:** Permite modificar o nome do arquivo.
  - **Excluir:** Remove o arquivo da lista.
  - **Aplicar também a subdiretórios:** Reforça as regras de proteção a arquivos para quaisquer subdiretórios de um diretório nomeado.
- **Ações restritas em arquivos protegidos**
  - **Acesso de leitura:** Evita que os programas especificados acima acessem os arquivos protegidos.
  - **Modificação:** Evita que os programas especificados acima façam quaisquer alterações nos arquivos protegidos.
  - **Criação:** Evita que os programas especificados acima criem os arquivos.
  - **Execução:** Evita que os programas especificados acima executem os arquivos protegidos.

Configurar parâmetros de firewall LANDesk

A nova ferramenta LANDesk Firewall é um componente importante da Segurança de ponto final que permite proteger os dispositivos gerenciados de operações e conexões de aplicativos não autorizados.

Com as configurações do LANDesk Firewall você pode criar e configurar programas confiáveis (aplicativos), escopos de rede confiável e regras de conexão para proteger dispositivos gerenciados de intrusões não autorizadas.

IMPORTANTE: Compatibilidade entre o LANDesk Firewall e Firewall do Windows
O LANDesk Firewall complementa o Firewall do Windows e ambos podem ser habilitados e serem executados ao mesmo tempo nos dispositivos gerenciados.

Componente de segurança de ponto final

O LANDesk Firewall é um dos componentes da solução abrangente de Segurança de ponto final juntamente com HIPS (Prevenção de intrusão no host) e as ferramentas de Controle de dispositivo.

Este capítulo contém informações sobre:

- "Uso das configurações do LANDesk Firewall" na página 696
- "Ajuda das configurações do LANDesk Firewall" na página 697

Uso das configurações do LANDesk Firewall

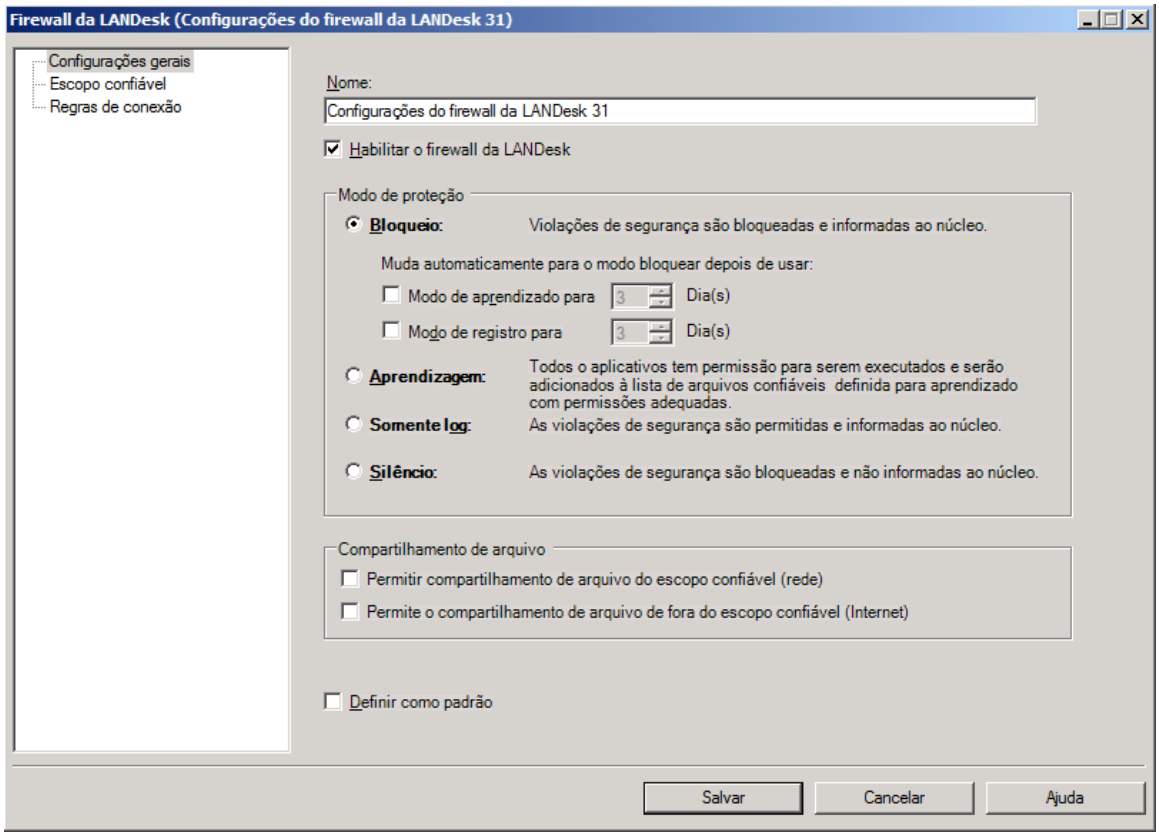
As configurações de firewall dão a você o controle completo sobre a forma com o LANDesk Firewall opera nos dispositivos alvo.

Esta seção descreve o modo de criar e gerenciar configurações de Firewall.

Criação das configurações do LANDesk Firewall

Para criar as configurações do LANDesk Firewall

1. Na janela da ferramenta **Configurações de agente**, clique com o botão direito em **LANDesk Firewall** e clique em **Novo**.


Firewall da LANDesk (Configurações do firewall da LANDesk 31)
Configurações gerais
Escopo confiável
Regras de conexão
Nome:
Configurações do firewall da LANDesk 31
Habilitar o firewall da LANDesk
Modo de proteção
Bloqueio:
Violações de segurança são bloqueadas e informadas ao núcleo.
Muda automaticamente para o modo bloquear depois de usar:
Modo de aprendizado para
3
Dia(s)
Modo de registro para
3
Dia(s)
Aprendizagem:
Todos o aplicativos tem permissão para serem executados e serão adicionados à lista de arquivos confiáveis definida para aprendizado com permissões adequadas.
Somente log:
As violações de segurança são permitidas e informadas ao núcleo.
Silêncio:
As violações de segurança são bloqueadas e não informadas ao núcleo.
Compartilhamento de arquivo
Permitir compartilhamento de arquivo do escopo confiável (rede)
Permite o compartilhamento de arquivo de fora do escopo confiável (Internet)
Definir como padrão
Salvar
Cancelar
Ajuda

2. Na página **Configurações gerais**, digite um nome para as configurações, habilite o serviço LANDesk Firewall e em seguida especifique o modo de proteção. Clique em **Ajuda** para encontrar mais informações sobre uma opção.
3. Na página **Listas de arquivos confiáveis**, adicione e edite os arquivos executáveis dos aplicativos que podem conectar com e a partir da rede local e da Internet. Também é possível exibir o escopo confiável.
4. Na página **Regras de conexão**, defina as regras de conexão (de entrada ou de saída e a ação) por porta, protocolo ou faixa de IP.
5. Clique em **Salvar**.

Uma vez configuradas, você poderá distribuir as configurações para dispositivos alvo com uma tarefa de instalação ou de atualização ou uma tarefa de mudança de configurações.

Ajuda das configurações do LANDesk Firewall

Use esta caixa de diálogo para criar e editar configurações do LANDesk Firewall. Ao criar configurações de Firewall defina primeiro o modo de proteção geral e, em então adicione e configure listas de arquivos confiáveis específicos, escopos confiáveis e regras de conexão. Você pode criar quantas configurações desejar e editá-las a qualquer momento.

Se desejar modificar as configurações padrão sem reinstalar a Segurança de ponto final ou distribuir uma configuração de agente completa, faça as modificações desejadas em qualquer uma das opções da caixa de diálogo, atribua as novas configurações a uma tarefa de mudança de configurações e distribua essa tarefa para os dispositivos alvo.

Este diálogo contém as seguintes páginas.

Sobre a página Configurações gerais

Use essa página para habilitar o LANDesk Firewall e configurar o modo de proteção.

Essa página contém as seguintes opções:

- **Nome:** Identifica as configurações de Firewall com um nome exclusivo.
- **Habilitar o LANDesk Firewall:** Permite a todos os programas serem executados (exceto quando a operação de um programa ameaça a segurança do sistema) como definidos nas regras de proteção pré-definidas.
- **Modo de proteção:** Especifica o comportamento de proteção quando ocorrem violações de segurança em dispositivos gerenciados.
    - **Modo automático:** todas as violações de segurança são bloqueadas automaticamente. Em outras palavras, todos os programas confiáveis, o escopo confiável e regras de conexão (ou seja, permissões) que foram criadas e impostas.
        - **Use o modo de aprendizado para:** Permitir que o administrador especifique um período de tempo durante o qual o usuário final pode executar qualquer aplicativo na máquina. Durante esse período, os aplicativos executados são observados.

          NOTA: Essas duas opções de período são executadas com sucessivamente. Em outras palavras, se ambas forem selecionadas, o período de aprendizado será executado primeiro até o fim, quando o período de modo de monitoramento será iniciado.

        - **Use o modo de monitoramento para:** Especificar um período durante o qual os aplicativos que são executados são gravados em um arquivos de histórico de ação no servidor núcleo.
    - **Modo de aprendizagem:** Todos os aplicativos podem ser executados. Além disso, todos os aplicativos que estão executando no dispositivo são aprendidos e adicionados à lista de arquivos confiáveis.
    - **Modo de monitoramento:** As violações de segurança são permitidas, mas são gravadas em um arquivo de histórico de ações no servidor núcleo.
    - **Modo bloquear:** As violações de segurança são bloqueadas, mas são gravadas em um arquivo de histórico de ações no servidor núcleo.

- **Compartilhamento de arquivos:** Especifica os privilégios de compartilhamento de arquivos permitido pelas configurações do LANDesk Firewall.
  - **Permite o compartilhamento de arquivo a partir de um escopo confiável (rede):** Permite que arquivos sejam compartilhados dentro do escopo confiável que você definiu.
  - **Permite o compartilhamento de arquivos a partir de um escopo externo confiável (rede):** Permite que arquivos sejam compartilhados fora do escopo confiável que você definiu.

Sobre a página Lista de arquivos confiáveis

Use esta página para criar e gerenciar listas de arquivos e escopos confiáveis.

Essa página contém as seguintes opções:

- **Listas de arquivos confiáveis:** Exibe a lista de arquivos com permissões configuradas para HIPS.
  - **Adicionar:** Abre a caixa de diálogo Configurar a lista de arquivos confiáveis, a partir de onde você pode gerenciar as listas de arquivos confiáveis.
  - **Editar:** Permite editar a lista de arquivos confiáveis selecionada.
  - **Remover:** Exclui a lista de arquivos confiáveis selecionada.
- **Opções de atividades de aprendizado:** Especifica como a atividade dos arquivos é manuseada quando o modo de proteção é definido como aprendizado.
  - **Lista de aprendizado:** Exibe a lista de arquivos confiáveis para o qual a atividade de arquivo de aprendizado é aplicada.
  - **Adicionar atividade de aprendizado somente na lista de aprendizado:** Limita a atividade do arquivo de aprendizado a ser aplicado somente a lista de arquivos especificados.
  - **Adicionar atividade de aprendizado em cada lista onde o mesmo arquivo já existe:** Permite que a atividade de arquivo de aprendizado seja aplicada a qualquer lista de aquivos que contenha aquele arquivo.
- **Escopo confiável:** Contém os escopos de rede que têm regras de conexão configuradas para proteção de firewall.

Sobre a caixa de diálogo Configurar aplicativo confiável

Use essa página para configurar as regras de conexão de um aplicativo específico.

Essa página contém as seguintes opções:

- **Detalhes do aplicativo:** Identifica o aplicativo ao qual as regras de conexão estão sendo atribuídas (exemplo, permissões). Você pode inserir uma descrição do arquivo.
- **Conexão de saída**
  - **Permite ao aplicativo conectar-se ao escopo confiável (rede):** Permite ao aplicativo conectar-se a locais dentro do escopo confiável que você definiu.
  - **Permitir ao aplicativo conectar-se fora do escopo confiável (Internet):** Permite ao aplicativo conectar-se a locais fora do escopo confiável que você definiu.
- **Conexão de entrada**
  - **Permitir ao aplicativo receber conexões do escopo confiável (rede):** Permite ao aplicativo receber conexões de locais dentro do escopo confiável que você definiu.
  - **Permitir ao aplicativo receber conexões de fora do escopo confiável (Internet):** Permite ao aplicativo receber conexões de locais fora do escopo confiável que você definiu.

- **Aplicativo confiável bloqueado:** Assegura que o aplicativo retenha as regras de conexão aqui atribuídas, mesmo se o aplicativo tiver permissão para executar outras operações duranta o modo de aprendizagem.
- **OK:** Salva as regras de conexão eadiciona o aplicativo à lista de programas confiáveis.
- **Cancelar:** fecha a caixa de diálogo sem salvar.

Sobre a caixa de diálogo Escopo confiável

Use essa página para configurar e gerenciar os escopos gerenciados. Um escopo confiável é composto de uma coleção de endereços de rede, por endereço de IP, faixa de IP ou sub-rede.

Essa página contém as seguintes opções:

- **Sub-rede do cliente confiável:** Adiciona a faixa da sub-rede do dispositivo alvo à lista de escopo confiável. É permitida a comunicação naquela faixa de sub-rede.
- **Escopos confiáveis:** Contém todos os escopos confiáveis.
- **Importar:** Permite importar faixas de sub-redes dos dispositivos gerenciados contido no inventário de banco de dados núcleo.
- **Adicionar:** Permite adicionar um local confiável à lista. Adicione um local confiável por endereço IP, faixa de IP ou sub-rede.
- **Editar:** Permite modificar o local confiável existente.
- **Excluir:** Remove os locais confiáveis selecionados.

Sobre a caixa de diálogo Regras de conexão

Use esta página para ver, gerenciar e priorizar regras de conexão. As regras de conexão podem permitir ou impedir conexões com base na porta ou na faixa de IP, seja o programa confiável ou não e esteja a comunicação dentro do escopo da rede confiável ou não.

Essa página contém as seguintes opções:

- **Regras de conexão:** Contém todas as regras de conexão.
- **Mover para cima:** Determina a prioridade da regra de conexão. Uma regra de conexão em posição mais alta na lista tem precedência sobre uma regra em posição mais baixa na lista.
- **Mover para baixo:** Determina a prioridade da regra de conexão.
- **Redefinir:** Restaura a ordem da regra.
- **Adicionar:** Abre um diálogo em que você pode configurar uma nova regra de conexão.
- **Editar:** Permite modificar a regra de conexão selecionada.
- **Excluir:** Remove a regra de conexão do banco de dados.

Sobre a caixa de diálogo Configurar regra de conexão

Use esta página para configurar regras de conexão.

Essa página contém as seguintes opções:

- **Nome:** identifica a regra de conexão com um nome descritivo.
- **Portas:** Permite definir restrições de porta para a regra de conexão.
    - **Aplicar a estas portas locais:** Especifica as portas locais às quais a direção e a ação (selecionada abaixo) são aplicadas. Por exemplo, se for selecionada De entrada e Aceitar estiver selecionada, as conexões às portas locais especificadas aqui são permitidas.
    - **Aplicar a estas portas remotas:** Especifica as portas remotas às quais a direção e a ação (selecionada abaixo) são aplicadas.
- **Protocolo:** Especifica o protocolo de comunicação para as portas selecionadas.
- **Faixa de IP:** Permite definir restrições de faixa de IP para a regra de conexão.
    - **Aplicar a estes endereços remotas:** Especifica a faixa de endereços IP remotos aos quais a direção e a ação (selecionada abaixo) são aplicadas.
- **Direção:** Indica se a regra de conexão restringe conexões de entrada ou de saída.
- **Ação:** Indica se a regra de conexão permite (aceites) ou impede conexões (desconexões).
- **Permitir programas confiáveis ignorar:** Permite dar aos programas confiáveis a capacidade de ignorar esta regra de conexão.
    - **Somente para escopo confiável:** Limita a capacidade dos programas confiáveis de ignorar a regra de conexão somente se a comunicação for dentro do escopo confiável da rede.
- **OK:** Salva as opções e adiciona a regra à lista de regras de conexão.
- **Cancelar:** fecha a caixa de diálogo sem salvar.

Controle de dispositivo

A nova ferramenta Controle de dispositivo é um componente importante da Segurança de ponto final que permite que o monitoramento e a restrição de acesso em dispositivos de E/S. Com o Controle de dispositivo você pode restringir o uso de dispositivos que permitem acesso de dados a dispositivos como portas, modem, unidades de disco e conexões sem fio.

Para implementar o Controle de dispositivo em clientes na sua rede, você cria e distribui configurações de controle de dispositivo que gerencia USB, modem, porta de E/S, unidade CD/DVD, PCMCIA e outras conexões.

Você pode configurar restrições a USB bloqueando de forma genérica uma classe inteira de dispositivos USB como, por exemplo, dispositivos de armazenamento ou usando configurações avançadas para restringir certos dispositivos USB baseados nos parâmetros e valores que especificar.

Componente de segurança de ponto final

O Controle de dispositivo é um dos componentes da solução abrangente de Segurança de ponto final juntamente com HIPS (Prevenção de intrusão no host) e as ferramentas LANDesk Firewall.

Plataformas suportadas

Controle de dispositivo suporta dispositivos gerenciados que executam:

- Windows 2000
- Windows Server 2003
- Windows XP
- Windows Vista (32 bits e 64 bits)
- Windows 7

Restringir acesso de dispositivos com as configurações de Controle de dispositivos

Para o Controle de dispositivo funcionar num dispositivo, é necessário que o agente agendador local e o agente distribuídos para aquele dispositivo. Cada vez que o dispositivo inicia uma conexão de dispositivo ou efetua mudanças a um dispositivo, o agente aplica as regras de configuração. Essas regras incluem o término de conexões que não são permitidas e o envio de alertas ao servidor núcleo.

Como padrão, as configurações de controle de dispositivo podem restringir os vários tipos de dispositivos. Você pode usar os parâmetros avançados de USB para restringir qualquer dispositivo USB ou classe de dispositivos que especificar. Entre os dispositivos que você pode restringir, estão:

- Dispositivos USB como, por exemplo, unidades de disco, teclados, mouse, impressora e scanners
- Dispositivos de mão RIM Blackberry, Pocket PC e Palm
- Volumes de rede
- Redes de área pessoal Bluetooth
- Redes sem fio 802.11x
- Modems
- Dispositivos PCMCIA
- Portas seriais, paralelas, infravermelhas e FireWire 1394
- Disquete e unidades de CD/DVD

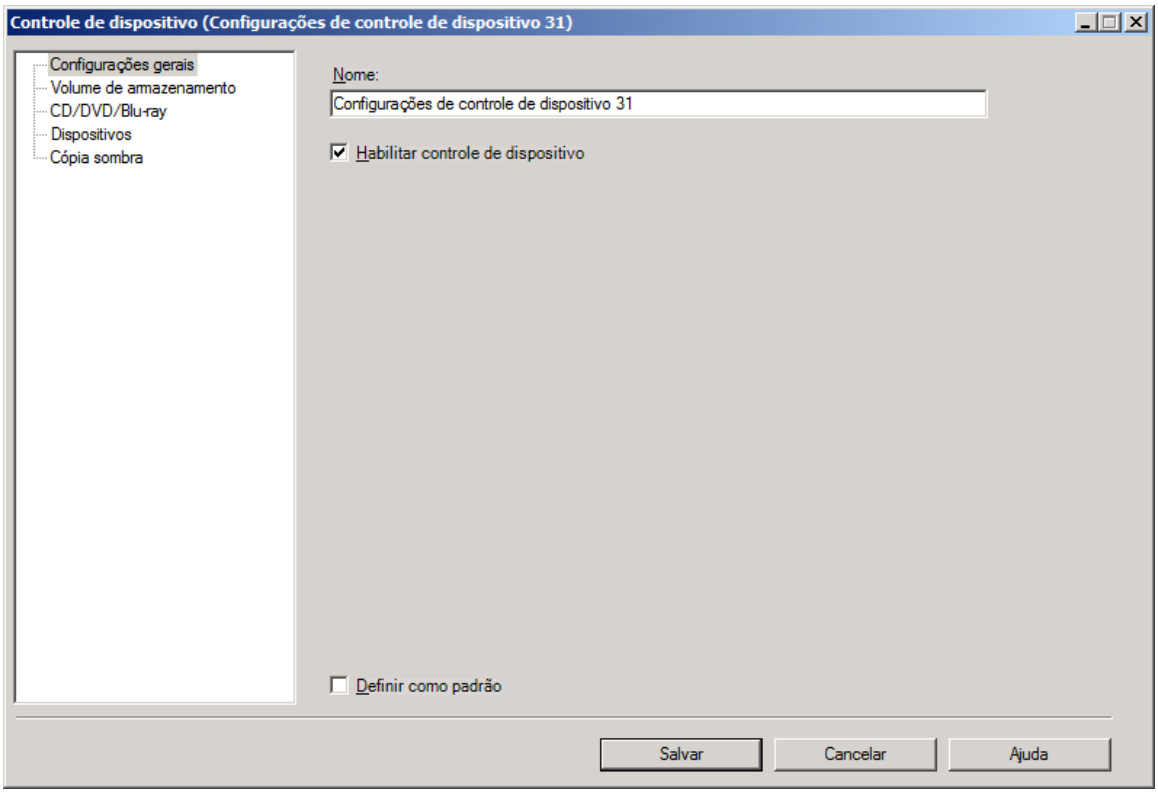
A configuração de controle de dispositivo USB usa o serviço LANDesk Endpoint Security, que pode:

- Impedir o uso de dispositivos USB e PCMCIA não autorizados.
- Impedir o uso de dispositivos removíveis de armazenamento não autorizados.
- Disparar um programa ou script externo ao detectar um dispositivo não autorizado.

Criar configurações de controle de dispositivo

Para criar configurações de controle de dispositivo

1. Clique em **Ferramentas > Segurança > Configurações de segurança**.
2. Abra Segurança de ponto final, clique com o botão direito em **Controle de dispositivo** e clique em **Novo**.



3. Na página Configurações gerais,digite um **Nome**.
4. Desmarque a caixa de seleção **Habilitar** controle de dispositivo.
5. Nas outras páginas, personalize as opções que quiser. Para obter mais informações sobre as opções na caixa de diálogo, consulte "Ajuda das configurações do Controle de dispositivo" na página 708.
6. Clique em **Salvar** para salvar as configurações.

Distribuir configurações de Controle de dispositivos

Após ter criado uma Configuração de controle de dispositivo é necessário distribuí-la para os dispositivos gerenciados antes de ser ativada.

O Controle de dispositivo é distribuído através das configurações de Segurança de ponto final.

Para distribuir configurações de controle de dispositivo

1. Clique com o botão direito em configurações e clique em **Agendar**.
2. A configuração é acrescentada à janela **Tarefas agendadas**. Nesta janela, arraste os dispositivos para o ícone configurações.
3. Quando todos os dispositivos tiverem sido adicionados, no menu de atalho da tarefa, clique em **Propriedades**. Na árvore, clique em **Agendar tarefa** e configure as opções de agendamento.

Para obter mais informações sobre agendamento de tarefas, consulte "Agendamento de tarefas" na página 227.

Ao agendar as configurações de controle de dispositivo para distribuição, o gerenciador de Controle de dispositivo faz o seguinte:

- Cria um pacote de distribuição executável nomeado com base da origem das configurações de controle de dispositivo. O arquivo primário do pacote é o ldsecsvc.exe. Os arquivos adicionais são ldsecsvc.reg, devactalert.exe, netres.mrl e <<*nome das configurações de controle de dispositivo*>.ini.
- Se você selecionar usuários como alvo para a tarefa de configurações do controle de dispositivo, o Controle de dispositivo usa um método de distribuição com base em diretiva denominado "Entrega por recepção do LANDesk Endpoint Security". Se esse método de distribuição não existir, o gerenciador de Controle de dispositivo o cria. Quando são usadas tarefas alvos, o gerenciador de Controle de dispositivo tem que usar um método de distribuição com base em diretiva para garantir que o usuário correto obtenha as configurações. Quando usuários alvos se conectam, o método de distribuição com base em diretiva ativa e instala as configurações.
- Se você selecionar computadores como alvo para a tarefa de configurações, o gerenciador de Controle de dispositivo usa um método de distribuição por envio suportado por diretiva com base em diretiva denominado "Entrega por envio do LANDesk Endpoint Security". Se esse método de distribuição não existir, o gerenciador de Controle de dispositivo o cria. As configurações selecionam um dispositivo como alvo, por isso, qualquer usuário que acessar o dispositivo obterá essas configurações de controle de dispositivo, independente de quem faz o login quando as configurações são instaladas. Você pode usar os métodos de distribuição por envio ou diretiva para computadores.

Assim que o gerenciador de Controle de dispositivo cria o método de distribuição por recepção com base em diretiva ou método de distribuição por envio com base em diretiva, você pode personalizá-los. Desde que o nome do método não mude, o gerenciador de Controle de dispositivo usará o método de entrega modificado.

Criar mensagens personalizadas quando dispositivos não autorizados forem detectados

No diálogo **Configurações de controle de dispositivo**, personalize o texto de mensagem que o usuário verá quando forem detectados dispositivos ou volumes. No texto da mensagem, você pode usar os marcadores a seguir, para mostrar informações sobre o volume ou dispositivo não autorizado:

- %vol%: número de série do sistema
- % desc % : descrição
- % serviço % : serviço
- %hwid%: ID de hardware
- % mfg % : fabricante
- % loc % : localização
- % class % : classe

Outras tarefas de gerenciamento de controle de dispositivo

Consulte esses tópicos relacionados para ver informações sobre as seguintes características e tarefas do Controle de dispositivos:

- Lidando com dispositivo não autorizado
- Como lidar com o dispositivo removível de armazenamento
- Configuração dos parâmetros avançados de USB
- Configuração de comandos que são executados quando um dispositivo não autorizado é detectado
- Configurar de alertas de Controle de dispositivos
- Visuzalizar a lista de dispositivos não autorizados

Lidando com dispositivo não autorizado

As configurações de controle de dispositivo usam o serviço LANDesk Endpoint Security em dispositivos gerenciados. Quando o serviço recebe notificação do SO que um novo USB ou dispositivo PCMCIA foi inserido, o serviço aplica um número de regras personalizadas, definidas, para decidir se o dispositivo é permitido ou não. É possível configurar regras simples para permitir somente determinados tipos de dispositivos, como, por exemplo, teclados e mouses, impressoras e scanners. Regras mais complexas podem permitir dispositivos somente de armazenamento de um dado fabricante ou excluir dispositivos de um outro.

Quando for detectado um dispositivo não autorizado, o serviço LANDesk Endpoint Security irá:

- Remover o dispositivo do Gerenciador de dispositivos do Windows para o Windows não o detectar mais. Os drivers do dispositivo continuam instalados.
- No caso de um dispositivo USB ou volume não autorizado, é mostrada uma mensagem opcional ao usuário. Para obter mais informações, consulte Criação de mensagens personalizadas quando os volumes/dispositivos não autorizados forem detectados.
- Você também pode carregar um programa externo (para mais informações, consulte Configuração de comandos que são executados quando um dispositivo não autorizado é detectado). O programa externo pode ser, por exemplo, um script que envia um alerta ao console central.
- Enviar um alerta AMS "Dispositivo desabilitado ativado" para o servidor núcleo. A mensagem de alerta inclui o nome do dispositivo.

Como lidar com o dispositivo removível de armazenamento

As conexões USB nos dispositivos gerenciados são restringidos por um serviço denominado LANDesk Endpoint Security Quando um novo volume é montado, o serviço recebe uma notificação do sistema operacional. O serviço , então, usa a chamada GetDriveType() API para verificar o tipo de unidade montada. Se o SO descrever a unidade como "removível" ou "fixa", o serviço agirá. O serviço também procura volumes removíveis na inicialização. Se for encontrado um volume não autorizado na inicialização, serão executadas as mesmas ações que aquelas executadas quando o volume é montado em outra hora.

As unidades consideradas como removíveis são os dispositivos de armazenamento USB (mas não estão limitadas aos mesmos). Unidades de CD (de apenas leitura ou leitura/gravação) não são considerados armazenamento removível.

O SO não considera os discos rígidos como removíveis. A chamada GetDriveType() os descreve como "unidades fixas" mesmo se estiverem anexados através de USB ou de outra porta externa. Para permitir que discos rígidos removíveis sejam manipulados da mesma maneira que outros dispositivos removíveis de armazenamento, o serviço registra a lista de discos rígidos no momento em que o serviço é instalado. Por exemplo, se um dispositivo tiver dois discos rígidos (C: e D:) quando o serviço for instalado, ele considerará essas unidades como fixas e não as verificará. Mas se, mais tarde, um disco rígido com a letra de unidade E: for encontrado, o serviço o considerará como dispositivo removível.

O serviço LANDesk Endpoint Security mantém a lista de "unidades fixas" no registry, no caminho HKLM\Software\LANDesk\usbmon\FixedDrives. Esta lista é criada na hora em que o serviço é instalado. A opção **Sem acesso** bloqueia o acesso a qualquer volume que não estava presente quando as configurações de controle do dispositivo foram instaladas. Observe que se um dispositivo que contém um volume tiver sido conectado quando as configurações foram instalada, o serviço dará permissão àquele dispositivo no futuro, muito embora ele seja removível.

Quando um dispositivo removível é detectado, o serviço LANDesk Endpoint Security irá:

- Bloquear o volume. Os usuários que tentarem acessar o volume receberão um erro de "acesso negado".
- Mostrar (opcionalmente) uma mensagem configurável ao usuário.
- Carregar (opcionalmente) um programa externo. O programa externo pode ser, por exemplo, um script que envia um alerta ao console central.
- Enviar um alerta AMS "Dispositivo desabilitado ativado" para o servidor núcleo. O alerta indica que foi ativado um volume, mas as informações adicionais sobre ele não estão disponíveis.

IMPORTANTE: O bloqueio de todos os volumes desconhecidos só funciona no Windows XP ou no Windows 2003
No Windows 2000, o sistema operacional indica que o volume está bloqueado quando esse não é o caso. Nós recomendamenos o bloqueio dos dispositivos específicos no Windows 2000 para impedir a adição de novos volumes.

O que acontece se uma pessoa do suporte precisar usar um memory stick USB?

Se você for uma pessoa de suporte de TI e quiser usar um dispositivo de armazenamento USB em computador de usuário, há várias coisas que podem ser feitas:

- O método temporário mais conveniente de permissão de acesso a um dispositivo USB é habilitar a opção de substituição de senha ao definir e distribuir configurações de controle de dispositivo nos dispositivos gerenciados.

Se o controle de dispositivo não estiver configurado com o recurso de substituição de senha, tente os seguintes métodos:

- Acesse com permissão de administrador e desative temporariamente o serviço LANDesk Endpoint Security.
- Acesse com permissão de administrador, abra a GUI do LANDesk Endpoint Security e adicione o dispositivo à lista de volumes autorizados.

Configurar de parâmetros avançados de USB

Após a instalação do gerenciador de controle de dispositivo em um dispositivo, o agente armazena informações sobre os últimos dez dispositivos USB aos quais foi bloqueado o acesso. O analisador de inventário envia essas informações ao banco de dados núcleo. As informações sobre esses dispositivos bloqueados aparecem então na caixa de diálogo **Configurações avançadas de USB**. Você pode usar essas informações para criar regras avançadas que permitem ou bloqueiam dispositivos USB específicos. Essas regras avançadas permitem controlar mais de uma categoria de dispositivos básicos mostradas na caixa de diálogo **Configurações de controle de dispositivo**.

Na caixa de diálogo **Configurações avançadas de USB**, você pode basear uma regra em qualquer das seis colunas. Clique com o botão direito em um valor na coluna e clique em **Permitir** para criar uma regra que permita dispositivos baseados nesse atributo. As palavras-chave criadas para cada uma dessas colunas são as seguintes:

```
DeviceDesc
HardwareID
Serviço
Mfg
LocationInformation
Classe
```

Esses são os mesmos nomes utilizados no registro na chave HKLM\System\CurrentControlSet\Enum\USB.

O campo mais útil onde se basear as regras, em geral, é **Serviço**. Isso corresponde a um driver do Windows. Por exemplo, o driver para as conexões USB ActiveSync para PDAs Windows CE é denominado wceusbsh (consulte a entrada HKLM\CurrentControlSet\Services\wceusbsh). Qualquer das seis colunas podem ser usadas para basear uma regra e você decide que regras são adequadas para a sua situação.

Curingas

Você pode usar caracteres curinga em regras. Por exemplo, o seguinte permitiria qualquer dispositivo com a string "floppy" em sua descrição de dispositivo:

```
DeviceDesc=*floppy*
```

Regras de lista branca x lista negra

Todas as regras ilustradas até o momento são regras de lista branca onde os dispositivos são proibidos a menos que satisfaçam pelo menos uma das regras. O serviço LANDesk Endpoint Security é compatível com regras de lista negra. As regras com prefixo de um sinal de subtração são regras de lista negra. Por exemplo:

```
Service=usbstor
-DeviceDesc=*floppy*
```

A primeira regra permite dispositivos de armazenamento USB. A segunda regra coloca nas listas negras, os dispositivos que contêm a string "floppy" na descrição de dispositivo.

Se as regras de lista branca e lista negra forem, ambas, definidas, o serviço compara primeiro os dispositivos com as regras de lista branca. Se não houver regras de lista branca que permitam o dispositivo, o dispositivo é proibido. Se houver pelo menos uma regra de lista branca que permita o dispositivo, então o serviço compara o dispositivo com as regras de lista negra. Se o dispositivo não satisfizer nenhuma regra da lista negra, ele é permitido. Caso contrário, ele é proibido.

Se existirem apenas as regras de lista branca, o dispositivo é proibido a menos que satisfaça uma das regras dessa lista. Se existirem apenas as regras de lista negra, o dispositivo é permitido a menos que satisfaça uma das regras dessa lista.

Regras compostas

Todas as regras ilustradas até agora são regras simples, onde é testado só um campo. O LANDesk Endpoint Security também é compatível com regras compostas, como no seguinte exemplo::

```
Service=wceusbsh,DeviceDesc=*iPAQ*
```

Essa regra permite apenas dispositivos Windows CE que contenham a string IPAQ na descrição de dispositivo.

Também é possível regras compostas de lista negra. Exemplo:

```
Service=wceusbsh
-Service=wceusbsh,Mfg=*iPAQ*
```

As duas linhas acima permitem dispositivos Windows CE, com exceção daqueles que contenham a string IPAQ no campo do fabricante. As linhas acima são equivalentes à seguinte linha única:

```
Service=wceusbsh,-Mfg=*iPAQ*
```

Configurar comandos que são executados quando um dispositivo não autorizado é detectado

Quando o serviço LANDesk Endpoint Security detecta um volume ou um dispositivo não autorizado, ele pode executar programas externos. Você pode selecionar um ou dois marcadores nos comandos:

- %1 será substituído pelo "volume" ou "dispositivo", dependendo da detecção de um volume ou um dispositivo USB não autorizado.
- %2 será substituído pelo número de série do volume não autorizado ou pela string de identificação de um dispositivo não autorizado.

Por exemplo, quando os comandos a seguir são digitados:

```
wscript myscript.vbs %1 %2
```

O comando a seguir é iniciado:

```
wscript myscript.vbs volume "1234ABCD"
wscript myscript.vbs device "Y-E Data USB Floppy: Vid_057b&Pid_0000"
```

O serviço garante que apenas uma instância do script será executada ao mesmo tempo.

Para configurar comandos

1. Na configuração de controle do dispositivo, clique em **Comandos**.
2. Digite o comando que desejar.
3. Clique em **OK**.

Configurar de alertas de monitoramento de dispositivos

As configurações de Controle de dispositivo usam o sistema de gerenciamento de alerta para fazer os alertas. O gerenciador de Controle de dispositivo pode disparar alertas nos seguintes eventos:

- Erro de configuração
- Dispositivo desabilitado ativado
- Tentativa de conexão de rede restrita

- Tentativa de conexão de rede não relacionada
- Detectada sessão de rede não relacionada

Exibir a lista de dispositivos não autorizados

Em cada computador, o gerenciador de Controle de dispositivo armazena uma lista dos dez dispositivos não autorizados mais recentes que foram conectados.

É possível exibir essas informações na **Tela de rede** clicando em **Inventário** em um menu de atalho do dispositivo. Clique em **LANDesk Management (Gerenciamento do LANDesk) > Controle de dispositivo > Alerta**.

Solução de problemas de Controle de dispositivo

Esta seção contém informações sobre algumas situações possíveis que podem ocorrer com o Gerenciador de dispositivos e como resolvê-las.

- Cada nova configuração de Controle de dispositivo é salva como um arquivo de configuração e um arquivo de script nas seguintes pastas:
  - ldmain\ccmgr\name.cfg
  - ldmain\scripts\name.ini
- Se um script ou configuração já existirem com o mesmo nome dado às configuração existente, uma mensagem confirmando se você deseja sobrescrever o script ou a configuração existentes será exibida. Isso pode fazer com que um script de distribuição não relacionado, do mesmo nome, seja sobregravado.
- Ao inserir faixas de IP para restrições de rede, não restrinja o acesso à faixa de rede na qual está o servidor núcleo. Se os clientes acessarem uma rede restrita e o Controle de dispositivo desabilitar o acesso à rede, o mesmo só pode ser restaurado através de comunicação com o servidor núcleo. Se os dispositivos não puderem se comunicar com o servidor núcleo devido a uma restrição, o acesso à rede não poderá ser restaurado.
- Ao restringir o acesso a dispositivos de E/S, não restrinja aqueles que são hosts para adaptadores de rede. Se você restringir o acesso a dispositivos de E/S que são hosts a um adaptador de rede, o cliente não será mais capaz de acessar a rede. Por exemplo, restringir o acesso ao USB impede que quaisquer adaptadores de rede USB funcionem. Sem o acesso à rede, você não poderá atualizar as configurações de atualização àquele cliente.
- Se você selecionar as seguintes opções no Controle de dispositivo e o servidor núcleo não estiver disponível em uma rede relacionada, os clientes terão acesso irrestrito ao dispositivo de E/S enquanto estiverem na rede.
  - Limite de conexões a redes relacionadas
  - Permitir redes não listadas se não estiver conectado
  - Verificação da existência do servidor núcleo na rede
- Se a opção "Permitir redes não relacionadas se não estiver conectado" estiver selecionada e o agente não puder encontrar o núcleo em uma rede relacionada, ele assumirá que a rede não está relacionada. Nesse ponto, um acesso não pretendido pode ser concedido a dispositivos de E/S locais. Isso pode criar riscos de segurança. Assegure-se de que o servidor núcleo esteja disponível para impedir essa situação de risco.

Ajuda das configurações do Controle de dispositivo

Use esta caixa de diálogo para criar e editar configurações do Controle de dispositivo.

Esta caixa de diálogo contém as seguintes páginas:

Sobre a página Configurações gerais

Use esta página para nomear as configurações e habilitar o controle de dispositivo em um cliente configurado com as configurações.

- **Nome:** identifica as configurações. Esse nome aparece na janela principal do gerenciador de Controle de dispositivo.
- **Habilitar o controle de dispositivo:** Ative o Controle de dispositivo em um cliente configurado com as configurações.

Sobre a página Volumes de armazenamento

Use esta página para especificar opções para volumes de armazenamento que conectam a um cliente configurado com estas configuração.

- **Volumes de armazenamento:** Especifica o nível de acesso para qualquer volume de armazenamento que não estava presente no cliente quando a configuração for instalada. (Observe que se um dispositivo que contém um volume tiver sido conectado quando a configuração foi instalada, o serviço LANDesk Endpoint Security dará permissão àquele dispositivo no futuro, muito embora ele seja removível.
  - **Acesso completo:** Permite acesso de leitura e gravação em um volume de armazenamento que se conecta.
  - **Acesso de leitura apenas:** Permite aos usuários a leitura de um volume de armazenamento que se conecta.
  - **Força criptografia:** Impões a criptografia de arquivo em um volume de armazenamento que se conecta. Distribui um utilitário de criptografia que permite a criptografia de arquivo em um dispositivo de armazenamento conectando a um cliente com esta configuração. Os arquivos são criptografados quando forem gravados a um dispositivo de armazenamento e descriptografados quando forem lidos do dispositivo. O acesso é permitido somente ao fornecer a senha correta (Isto é definido ao criar uma pasta criptografada no dispositivo de armazenamento USB.

    IMPORTANTE: Primeiro crie uma pasta criptografada no dispositivo USB: Quando um dispositivo de armazenamento for configurado para a criptografia de arquivo, os usuários devem criar inicialmente uma pasta criptografada antes de poderem copiar arquivos com o utilitário de criptografia (vá para **Iniciar > LANDesk Management > LANDesk Encryption > Avançado > Criar pasta criptografada**). Especifique uma senha ao criar a pasta criptografada. Se a opção Permitir dicas de senha estiver habilitada (ver abaixo), o usuário terá a opção de digitar uma dica para ajudá-lo lembrar a senha, embora a dica de senha não é requerida.

  - **Se acesso:** Impede o uso de volumes de armazenamento que se conectam a um cliente configurado com esta configuração de controle de dispositivo. Você pode personalizar que tipos de dispositivos USB são ainda permitidos selecionando tipos de dispositivos na página Dispositivo.
- **Exceções:** Clique para criar exceções para o nível de acesso aos volumes de armazenamento. Você pode adicionar exceções baseadas em ID de hardware, mídia serial ou tipo barramento.

- **Opções de criptografia:**
  - **Espaço de armazenamento alocado para criptografia:** Especifica o máximo de espaço em um dispositivo de armazenamento que pode ser usado para arquivos criptografados.
  - **Permitir dicas de senha:** Permite ao usuário final digitar uma dica para ajudá-lo lembrar a senha da pasta criptografada. A dica de senha não pode ser uma correspondência exata da senha mesma. A dica de senha não pode exceder 99 caracteres de comprimento. (Note que mesmo se o campo da dica de senha estiver disponível para digitar texto, o usuário não é requerido digitar uma dica.)
- **Notificar usuários finais:** Mostra uma caixa de mensagem quando um usuário conecta-se a um dispositivo não autorizado. Para saber mais, consulte "Ajuda das configurações do Controle de dispositivo" na página 708.

Sobre Configurar a caixa de diálogo exceção (para volumes de armazenamento)

Use esta caixa de diálogo para criar uma exceção para o nível de acesso aos volumes de armazenamento.

- **Descrição:** Digite uma descrição que deseja para identificar esta exceção.
- **Parâmetro:** Selecione o tipo de parâmetro (ID de hardware, volume serial ou tipo de barramento).
- **Valor:** Se o parâmetro de ID for selecionado, digite uma string de valor.
- **Acesso:** Especifica o nível de acesso para esta exceção (acesso completo, acesso de apenas leitura, apenas criptografia sem acesso).

Sobre a página Dispositivos

Use esta página para especificar opções para tipos de dispositivo que conectam a um cliente configurado com esta configuração.

- **Dispositivos / Interfaces:** Use as caixas de seleção para bloquear dispositivos e interfaces para impedi-los de acessar o cliente.
- **Bloquear LAN sem fio 802.11X:** Bloqueia uma conexão sem fio LAN802.11X.
- **Exceções:** Clique para criar exceções para bloquear dispositivos e interfaces. Você pode adicionar exceções baseadas em hardware_id, class, service, enumerator, vendor_id, device_id, or vendor_ device_id.
- **Unidade de CD/DVD:** Especifica o nível de acesso para unidade de CD / DVD.
- **Exceções:** Clique para criar exceções para o nível de acesso à unidade de CD/DVD. Você pode adicionar exceções baseadas em ID de hardware, mídia serial ou tipo barramento.
- **Notificar usuários finais:** Mostra uma caixa de mensagem quando um usuário conecta-se a um dispositivo não autorizado.

Sobre Configurar a caixa de diálogo exceção (para volumes de armazenamento)

Use caixa de diálogo para criar uma exceção para bloquear dispositivos e interfaces.

- **Descrição:** Digite uma descrição que deseja para identificar esta exceção.
- **Parâmetro:** Selecione o tipo de parâmetro (ID de hardware, volume serial ou tipo de barramento).
- **Valor:** Se o parâmetro de ID for selecionado, digite uma string de valor.
- **Acesso:** Especifica o nível de acesso para esta exceção (acesso completo, acesso de apenas leitura, apenas criptografia sem acesso).

Sobre a página Cópia sombra

Use esta página para habilitar e configurar a cópia sombra nos dispositivos gerenciados configurados com esta configuração de agente.

A cópia sombra permite controlar que arquivos forma copiados para e do dispositivo fazendo uma cópia duplicada (ou sombra) desses arquivos em um diretório local.

- **Habilitar cópia sombra:** Ative a cópia sombra de dispositivo gerenciados com essa configuração.
- **Evento de log apenas:** Indica que apenas a atividade de cópia de arquivo é gravada em um arquivo de diálogo e não os arquivos que estão sendo copiados.
- **Exceções:** Clique para criar exceções. Você pode adicionar exceções baseadas em ID de hardware, mídia serial ou tipo barramento.
- **Cache local:** Especifica o local na unidade local onde os arquivos de cópia sombra são copiados e o arquivo de log é armazenado.

LANDesk Antivirus

Visão geral do LANDesk Antivirus

O LANDesk Antivirus é composto por um agente de análise antivírus integrado, por um banco de dados de assinaturas de vírus atualizado constantemente e por opções de configuração e recursos antivírus disponíveis na ferramenta de **Configurações de agente**.

IMPORTANTE: Agente Antivirus
O agente Antivirus é distinto do agente de análise de segurança Patch e Conformidade.

LANDesk Security SuiteOs serviços mantêm um banco de dados atualizado de arquivos de definição/padrões de vírus do qual pode ser feito download, e que pode ser avaliado, testado e distribuído para dispositivos alvo na sua rede LANDesk.

Com o LANDesk Antivirus é possível:

- Descarregar as atualizações mais recentes do arquivo de definições/padrões de vírus (o banco de dados de assinatura de antivírus dos serviços do LANDesk Security Suite é atualizado várias vezes ao dia)
- Agendar atualizações do arquivo de definição de vírus de forma recorrente
- Arquivar arquivos anteriores de definição de vírus
- Criar e distribuir tarefas de instalação do agente Antivirus
- Executar análises antivírus por demanda e agendadas em dispositivos alvo
- Configurar o comportamento da análise antivírus e as opções do usuário
- Selecionar os tipos de arquivos a serem analisados e se haverá análise para identificação de riskware
- Habilitar proteção contra vírus de arquivos e emails em tempo real
- Analisar para verificar a presença de mecanismos de análise de antivírus de terceiros, e habilitar/desabilitar análise de vírus em tempo real e assegurar a atualização de arquivos de padrões de vírus para os produtos antivírus específicos
- Exibir a atividade antivírus e as informações de status dos dispositivos analisados
- Configurar alertas de antivírus
- Gerar relatórios de antivírus

Tipos de conteúdo de segurança e assinaturas

Quando você instala o LANDesk Management Suite ou LANDesk Security Suite, a ferramenta Patch e Conformidade é incluída como padrão. Entretanto, sem uma assinatura de conteúdo do Security Suite, somente será possível analisar atualizações e definições personalizadas de software LANDesk. A assinatura de conteúdo do Security Suite permite aproveitar os recursos oferecidos pela ferramenta Patch e Conformidade (e ferramenta Configurações de segurança) fornecendo acesso a conteúdo adicional de segurança e patches (tipos de definições), incluindo regras de detecção para análise antivírus e arquivos de definição de vírus do LANDesk Antivirus usados pelo analisador.

Tipos de conteúdo de segurança incluem:

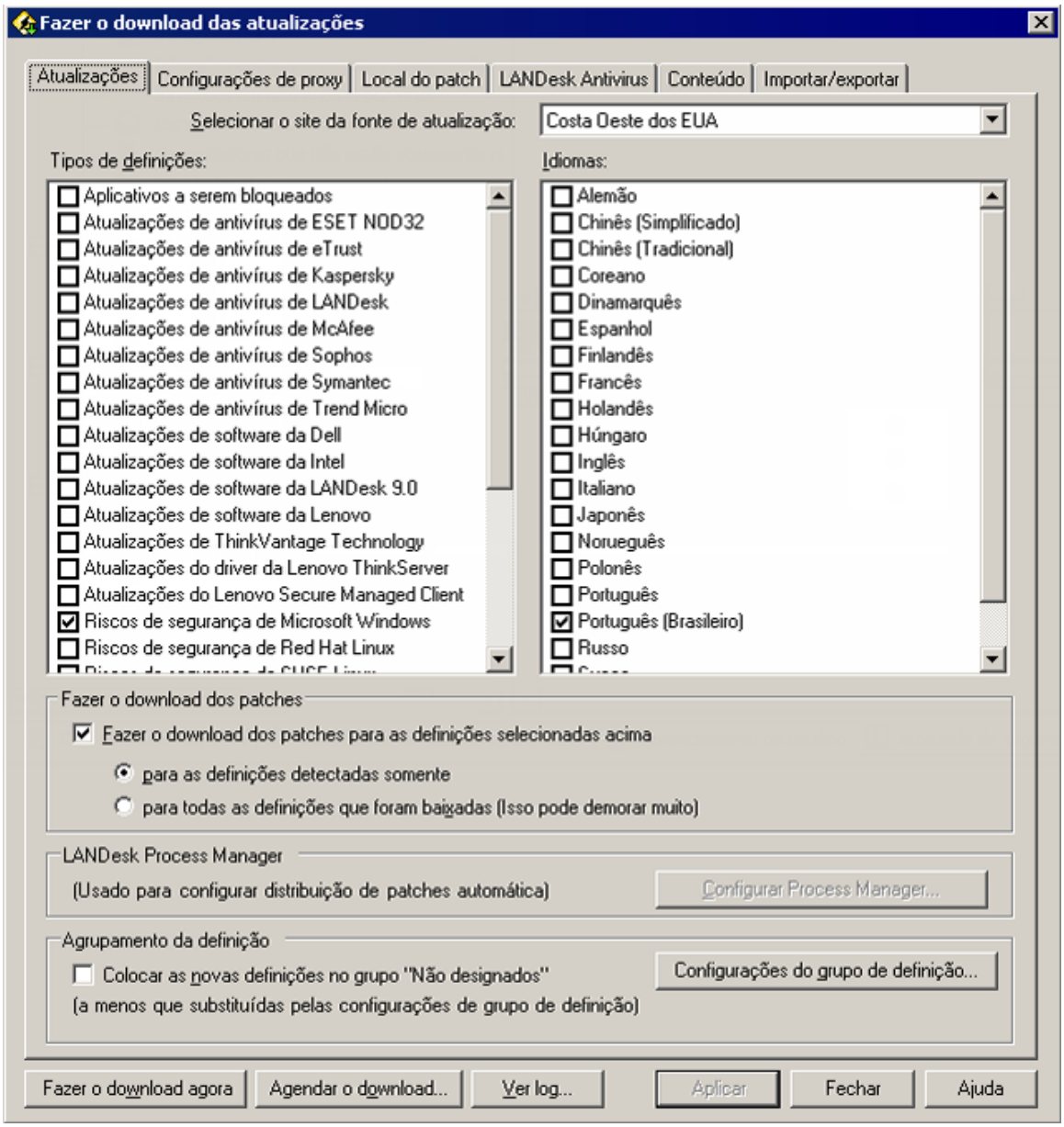
- Atualizações de antivírus (para analisadores de terceiros, inclui somente o conteúdo de detecção do analisador antivírus; para o Antivirus, inclui o conteúdo de detecção do analisador *e* os arquivos de definição de vírus, bem como arquivos de definição de riskware disponíveis em um banco de dados estendido)
- Aplicativos bloqueados (consulte "Isenção de responsabilidades legais para o tipo de aplicativos bloqueados" na página 581)
- Definições de vulnerabilidades personalizadas
- Atualizações de drivers
- Atualizações de software LANDesk
- Ameaças à segurança (exposições da configuração do sistema; inclui detecção e configuração de firewall)
- Atualizações de software
- Spyware
- Vulnerabilidades (vulnerabilidades conhecidas de plataformas e vulnerabilidades específicas de aplicativos)

Para obter informações sobre assinaturas de conteúdo, entre em contato com o representante da LANDesk ou visite o site da LANDesk:

LANDesk Home Page

Usando o Download de atualizações

Observe que a página **Atualizações** da caixa de diálogo **Fazer o download das atualizações** inclui várias atualizações de antivírus na lista de tipos de definição, incluindo uma denominada Atualizações do LANDesk Antivirus. Quando você seleciona Atualizações do LANDesk Antivirus, o conteúdo de detecção do analisador *e* as atualizações do arquivo de definições de vírus do LANDesk Antivirus são obtidos por download.



Para mecanismos de análise de terceiros, as atualizações de antivírus incluem definições do analisador que detectam:

- instalação de mecanismos de análise antivírus comuns (incluindo a ferramenta Antivirus)
- status de análise em tempo real (ativado ou desativado)
- versões do arquivo de padrões específicos do analisador (atualizado ou antigo)
- data da última análise (se a análise mais recente estiver dentro do período máximo permitido especificado pelo administrador)

Para o analisador do Antivirus, as atualizações de antivírus não apenas incluem o conteúdo de detecção do analisador indicado acima, mas também os arquivos de definição de vírus usados pelo analisador do LANDesk Antivirus.

NOTA: Conteúdo de detecção do analisador de antivírus comparado ao conteúdo de definições
As atualizações de antivírus não determinam a existência de arquivos de definição/padrões de vírus. Quando você faz o download das atualizações antivírus de terceiros, apenas o conteúdo de detecção do analisador é baixado para o repositório padrão, mas não os arquivos de definição de vírus específicos do analisador. Entretanto, quando você faz o download das atualizações do antivírus, o conteúdo de detecção do analisador e os arquivos de definições de vírus específicos do antivírus são baixados. Os arquivos de definição de vírus do Antivírus são baixados em um local separado no servidor núcleo. O repositório padrão do arquivo de definições de vírus é a pasta \LDLogon\Antivirus\Bases.

Plataformas de dispositivo com suporte

Para obter informações detalhadas atualizadas sobre quais plataformas de cliente são compatíveis com o LANDesk Antivirus, consulte o documento 'OS Compatibility Feature Matrix' na comunidade de usuários da LANDesk:

Página inicial da Comunidade de usuários da LANDesk

IMPORTANTE: Reinicialização necessária em computadores Windows NT 4.0
Para que o serviço do Antivírus seja ativado, os computadores com o Windows NT 4 devem ser reinicializados após a distribuição da configuração do agente.

Outros requisitos do sistema

Os dispositivos gerenciados que você for configurar com o agente Antivírus devem satisfazer os requisitos do sistema:

- Microsoft Internet Explorer 6.0 ou superior
- Nenhum outro produto antivírus instalado

Administração com base em funções com o LANDesk Antivirus

O LANDesk Antivírus, como o Patch e Conformidade, utiliza a administração baseada em funções para permitir o acesso dos usuários aos recursos. A administração com base em funções é a estrutura de acesso e segurança que permite aos administradores restringir o acesso a ferramentas e dispositivos. Cada usuário recebe funções e escopo específicos que determinam quais recursos podem usar e quais dispositivos podem gerenciar.

Os Administradores atribuem essas funções a outros usuários com a ferramenta Gerenciar usuários no console. Antivirus é incluso no direito Configurações de segurança que aparece sob o grupo de direitos de segurança na caixa de diálogo Funções. Para ver e usar os recursos do Antivirus, os direitos necessários de Configurações de segurança precisa ser atribuído ao usuário.

IMPORTANTE: Permissões de grupos LANDesk Script Writers são necessárias
Para criar tarefas agendadas e diretivas na ferramenta Patch e conformidade e a ferramenta Configurações de segurança (para tarefas de análise de segurança e conformidade, tarefas de reparo e tarefas de mudanças de configurações), um usuário precisa ter permissão de grupo LANDesk Script Writers. Em outras palavras, eles precisam pertencer a um grupo que tenha permissão de LANDesk Script Writers atribuída. Para obter mais informações sobre a administração baseada em funções, consulte

"Gerenciamento de usuários" na página 38.

Com o direito Configurações de segurança, você pode fornecer aos usuários a habilidade de:

- Distribuir configurações de agente com o Antivírus para os dispositivos alvo
- Fazer download de atualizações do arquivo de definições de vírus
- Criar atualizações agendadas
- Criar tarefas de análise antivírus agendadas
- Criar configurações de antivírus
- Distribuir tarefas de análise antivírus e alterar as tarefas de configuração associadas às configurações de antivírus
- Habilitar a proteção de arquivos e emails em tempo real
- Configurar análises antivírus para verificar tipos de arquivos específicos
- Excluir certos arquivos, pastas e tipos de arquivo (por extensão) das análises antivírus
- Ver a atividade antivírus e as informações de status dos dispositivos analisados
- Habilitar alertas de antivírus
- Gerar relatórios de antivírus (também requer funções de Relatórios)

Fluxo de trabalho da tarefa de antivírus

As etapas a seguir fornecem um resumo rápido dos processos ou tarefas típicas relacionadas à implementação da proteção antivírus na sua rede com o uso do LANDesk Antivirus. Cada um desses procedimentos é descrito em detalhes nas seções subseqüentes.

Etapas básicas para a implementação e uso do LANDesk Antivirus:

1. Configuração de dispositivos gerenciados para análise de antivírus.
2. Faça o download de atualizações de arquivo de definição/padrão de virus de um servidor de conteúdo de segurança.
3. Decisão sobre a disponibilização dos arquivos de definição de vírus para os dispositivos gerenciados imediatamente ou antes avaliá-los em um ambiente de teste piloto.
4. Criação de tarefas e diretivas de análise antivírus por demanda e agendadas.
5. Configure as definições de antivírus para determinar a operação de análise e opções do usuário final
6. Analise os dispositivos gerenciados para vírus conhecidos e arquivos suspeitos.
7. Veja os resultados da análise antivírus dos dispositivos analisados.
8. Configure alertas de antivírus.
9. Gere relatórios de antivírus

Configurar dispositivos com proteção Antivírus

Para procurar e limpar vírus em dispositivos gerenciados, o agente Antivírus deverá estar instalado nesses dispositivos. Você pode fazer isso durante a configuração inicial do agente no dispositivo ou com uma tarefa de instalação ou atualização separada.

Considerações sobre a distribuição do antivírus

Se você distribuir o Antivírus para um dispositivo que já tenha outra solução de antivírus instalada e em execução, ele não ativará sua funcionalidade de proteção em tempo real para evitar possíveis conflitos de software. Uma vez que o outro produto tenha sido removido, você poderá ativar a proteção em tempo real do Antivírus.

Você pode escolher remover automaticamente software antivírus existente dos dispositivos alvo ao distribuir o LANDesk Antivirus. Isso pode ser feito durante a configuração inicial do agente ou como tarefa separada de instalação/atualização do Antivirus. Os produtos antivírus que podem ser removidos dos dispositivos consulte "Lista de produtos antivírus de terceiros que podem ser removidos automaticamente" na página 717.

IMPORTANTE: Limpar software antivírus protegido por senha
Se o produto antivírus existente estiver protegido por senha, primeiro, você deverá limpá-la antes que o LANDesk Antivirus possa desinstalar o software.

Lista de produtos antivírus de terceiros que podem ser removidos automaticamente

Os seguintes são produtos antivírus que podem ser removidos automaticamente na distribuição (ou atualizando)LANDesk Antivirus:

- Symantec Antivirus (versões 7, 8, 9 e 10)
- Symantec Endpoint Protection 11
- McAfee Enterprise (versões 7.0, 8.0i, 8.5)
- McAfee ePolicy Orchestrator EPO
- Trend Micro PC-cillin (versões 2004, 2005, 2006, 2007 15.3 no Windows Vista 64-bit)
- Trend Micro OfficeScan
- Trend Micro ServerProtect
- Trend Micro Internet Security 2008
- CA eTrust Antivirus (versões 6, 7.x, 8, 8.1)

Configurar dispositivos com proteção Antivírus

Para configurar dispositivos com o Antivirus através da configuração do agente

1. No console, clique em **Ferramentas > Configuração > Configuração de agentes**.
2. Clique no botão da barra de ferramentas **Novas janelas**.
3. Após especificar as configurações desejadas para a configuração do agente, primeiro, é necessário clicar na página **Iniciar** e selecionar a opção **LANDesk Antivirus**. Agora, você pode acessar as opções na página **LANDesk Antivirus**.
4. Clique no grupo **Segurança e Conformidade** e clique em **LANDesk Antivirus**.
5. Se você quiser remover automaticamente um produto antivírus dos dispositivos alvo, selecione a opção **Remover agente antivírus existente**. Para ver a lista atual dos produtos antivírus que podem ser removidos dos dispositivos consulte "Lista de produtos antivírus de terceiros que podem ser removidos automaticamente" na página 717.

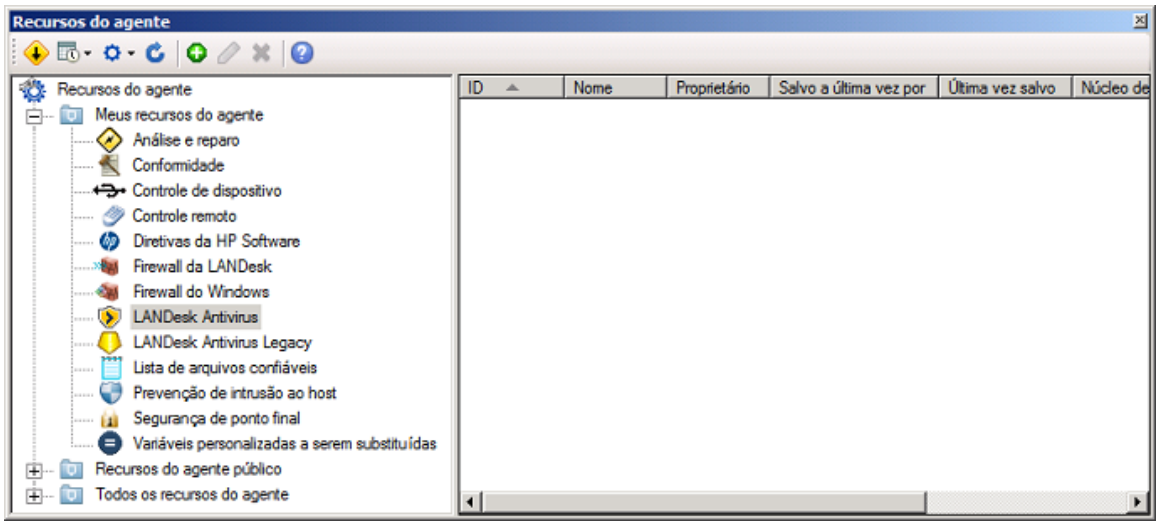
6. Selecione uma configuração de antivírus na lista disponível para aplicar à configuração do agente que está criando. Você pode criar novas configurações ou editar as configurações existentes clicando em **Configurar**. Configurações de antivírus determinam se o ícone Antivírus aparece na bandeja do sistema do dispositivo, disponibilidade de opções interativas para usuários finais, verificação de e-mail e ativação de proteção em tempo real, tipos de arquivos para verificar, arquivos e pastas para excluir, quarentena de arquivo infectado e Backup, verificação agendada de antivírus, e definições de atualizações de vírus agendados.
7. Termine de especificar outras definições para a configuração do agente e clique em **Salvar**.

Você pode também configurar dispositivos para o Antivirus com a ferramenta Configurações de segurança.

Uso da ferramenta Configurações de segurança

Se desejar instalar ou atualizar o Antivirus outra hora, você poderá fazê-lo como uma tarefa separada do console.

Use a ferramenta Configurações de segurança (**Ferramentas > Segurança > Configurações de segurança**) para criar tarefas de instalação ou atualização, tarefas de remoção e atualização de arquivo de definição de antivírus e tarefas de análise.



Para instalar ou atualizar o Antivirus como tarefa separada

1. No console, clique em **Ferramentas > Segurança > Configurações**.
2. Clique no botão **Criar uma tarefa** da barra de ferramentas e clique em **Instalar ou atualizar os componentes de segurança**.
3. Digite um nome para a tarefa.
4. Especifique se a instalação é uma tarefa agendada, baseada em diretivas ou ambas.
5. Selecione o componente que você quer instalar, neste caso, selecione o LANDesk Antivirus. Você pode selecionar uma configuração de antivírus na lista disponível para aplicá-la à tarefa que está criando. Você também pode criar novas configurações ou editar configurações existentes de antivírus.
6. Para mostrar o andamento da instalação na caixa de diálogo do analisador de segurança nos dispositivos alvo, selecione a opção **Mostrar diálogo de andamento no cliente**.

7. Se você quiser remover automaticamente um produto antivírus dos dispositivos alvo, selecione a opção **Remover agente antivírus existente**. Para ver a lista atual dos produtos antivírus que podem ser removidos dos dispositivos consulte "Lista de produtos antivírus de terceiros que podem ser removidos automaticamente" na página 717.
8. Selecione uma configuração de análise e reparo na lista disponível para aplicar sua configuração de reinicialização à tarefa que está criando. Você pode criar novas configurações ou editar as configurações existentes clicando em **Configurar**. A tarefa usará as opções de reinicialização das configurações de análise e reparo *somente*, o que determina os requisitos de reinicialização e as ações nos dispositivos alvo durante a instalação do agente do Antivirus.
9. Clique em **OK**.

Remover o LANDesk Antivirus dos dispositivos

Se você desejar remover o Antivírus dos dispositivos gerenciados e pode também fazer isso como uma tarefa separada.

Para remover o LANDesk Antivirus

1. No console, clique em **Ferramentas > Segurança > Configurações**.
2. Clique no botão **Criar uma tarefa** da barra de ferramentas e clique em **Remover componentes de segurança**.
3. Digite um nome para a tarefa.
4. Especifique se a instalação é uma tarefa agendada, baseada em diretivas ou ambas.
5. Para mostrar o andamento da instalação na caixa de diálogo do analisador de segurança nos dispositivos alvo, selecione a opção **Mostrar diálogo de andamento no cliente**.
6. Selecione uma configuração de análise e reparo na lista disponível para aplicar sua configuração de reinicialização à tarefa que está criando. Você pode criar novas configurações ou editar as configurações existentes clicando em **Configurar**. A tarefa usará as opções de reinicialização das configurações de análise e reparo *somente*, o que determina os requisitos de reinicialização e as ações nos dispositivos alvo durante a remoção do agente Antivirus.
7. Clique em **OK**.

Atualizar arquivos de definição de vírus

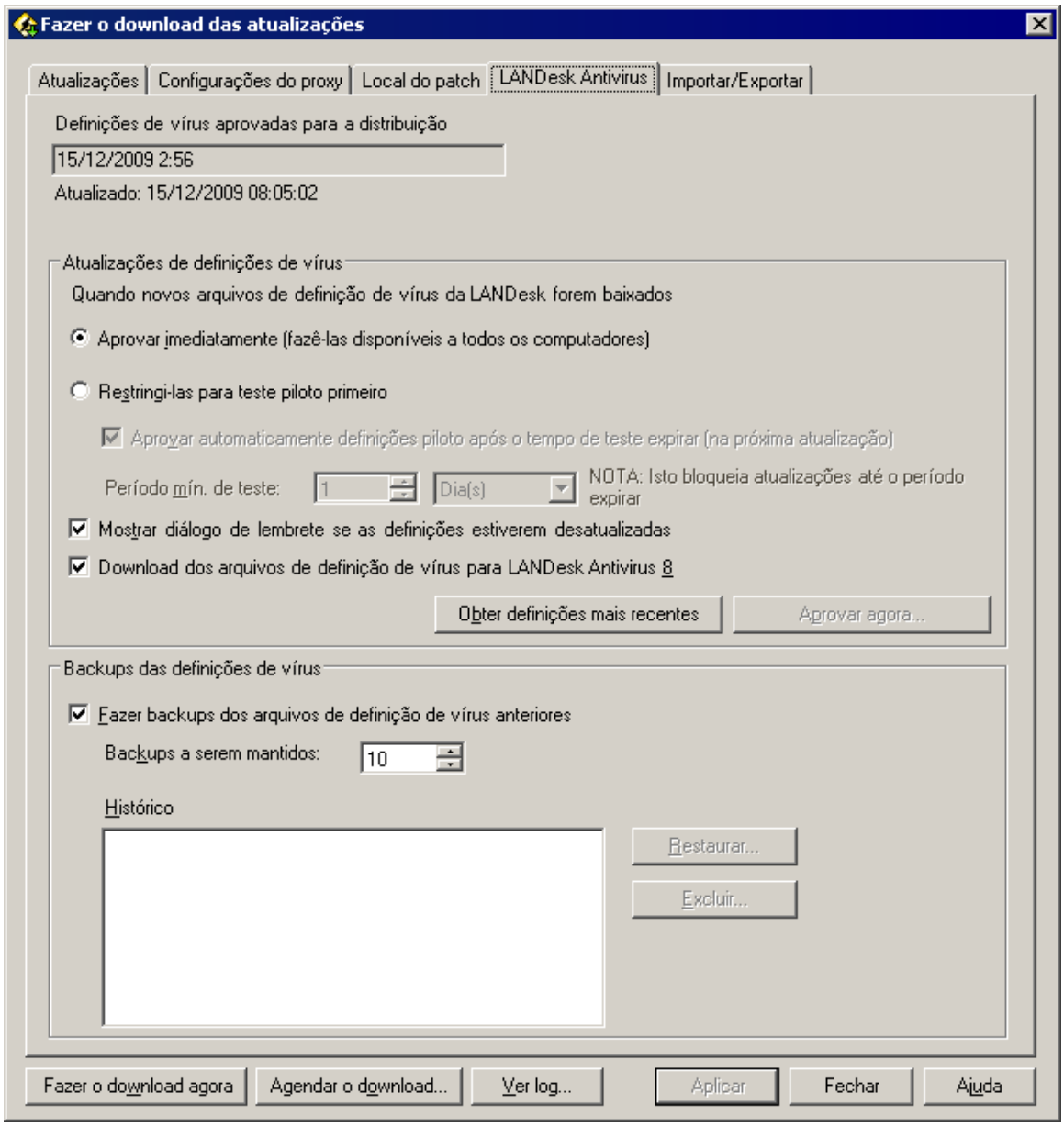
O Antivirus permite o download dos arquivos de definição de vírus mais recentes dos servidores de conteúdo do LANDesk Security Suite. O banco de dados de assinaturas de vírus é atualizado várias vezes ao dia a fim de garantir a disponibilidade das definições de vírus conhecidos mais recentes para proteger seus dispositivos gerenciados contra essas ameaças que evoluem tão rapidamente.

Você pode descarregar as atualizações do arquivo de definição de vírus do console, manualmente ou como uma tarefa única ou como uma tarefa agendada regularmente.

Uso do Download de atualizações para arquivos de definição de vírus

Use o Download de atualizações (**Configurações de segurança > Download de atualizações**) para especificar para onde os arquivos de definição serão copiados Eles podem ser armazenados no repositório padrão de arquivos de definição de vírus de onde serão distribuídos para dispositivos alvo ou se deverão ser copiados para um escopo limitado de dispositivos a fim de testá-los antes da distribuição.

Você também pode acessar esta caixa de diálogo diretamente quando criar uma tarefa de Antivírus.


Fazer o download das atualizações
Atualizações
Configurações do proxy
Local do patch
LANDesk Antivirus
Importar/Exportar
Definições de vírus aprovadas para a distribuição
15/12/2009 2:56
Atualizado: 15/12/2009 08:05:02
Atualizações de definições de vírus
Quando novos arquivos de definição de vírus da LANDesk forem baixados
Aprovar imediatamente (fazê-las disponíveis a todos os computadores)
Restringi-las para teste piloto primeiro
Aprovar automaticamente definições piloto após o tempo de teste expirar (na próxima atualização)
Período mín. de teste:
1
Dia(s)
NOTA: Isto bloqueia atualizações até o período expirar
Mostrar diálogo de lembrete se as definições estiverem desatualizadas
Download dos arquivos de definição de vírus para LANDesk Antivirus 8
Obter definições mais recentes
Aprovar agora...
Backups das definições de vírus
Fazer backups dos arquivos de definição de vírus anteriores
Backups a serem mantidos:
10
Histórico
Restaurar...
Excluir...
Fazer o download agora
Agendar o download...
Ver log...
Aplicar
Fechar
Ajuda

NOTA: Distribuição de arquivos de definição de vírus para dispositivos de usuários finais
As atualizações de definições de vírus descarregadas podem ser distribuídas aos dispositivos de usuários finais remotamente do servidor núcleo. Dos seus próprios computadores, os usuários também podem executar a tarefa de atualização dos arquivos de definição de vírus. Por padrão, eles fazem o download dos arquivos do seu servidor núcleo LANDesk. Entretanto, para poder fazer o download das últimas definições de vírus sem estar conectado à rede (por exemplo, em viagens ou no laptop), você pode fornecer a opção de deixar usuários fazerem o download diretamente do servidor de conteúdo do LANDesk Security Suite via Internet.

Para fazer download das atualizações do arquivo de definição de vírus

1. Clique em **Ferramentas > Segurança > Configurações de segurança**.
2. Clique no botão da barra de ferramentas **Fazer o download das atualizações**. A caixa de diálogo abre para a página **Antívirus**. (Você pode também acessar a caixa de diálogo **Download de atualizações** da ferramenta Patch e Conformidade.)
3. Na página **Atualizações**, selecione o site de origem das atualizações na lista de servidores de conteúdo disponíveis. Escolha aquele mais perto do seu local.
4. Nas páginas **Atualizações**, selecione **Atualizações do antivírus** na lista de tipos de definições. (É possível selecionar mais de um tipo de definição para um download. Entretanto, você deverá ter a assinatura correspondente do LANDesk Security Suite. Quanto mais tipos você selecionar, maior será o tempo necessário para a atualização.)
5. Na página **Atualizações**, selecione os idiomas cujo conteúdo você deseja atualizar para os tipos que especificar.
6. Se você desejar que o novo conteúdo (conteúdo que já não seja residente em nenhum grupo da árvore) seja colocado automaticamente no grupo Não atribuído em vez de no local padrão, que é o grupo Analisar, marque a caixa de seleção **Colocar as novas definições no grupo "Não designados"**.
7. Agora clique em **LANDesk Antivirus** para ver o status atual dos arquivos de definições de vírus e para configurar os parâmetros de atualizações específicas de vírus.
8. Se desejar que os arquivos de definições de vírus sejam descarregadas no repositório padrão no servidor núcleo (\LDLogon\Antivirus\Bases) onde eles podem ser distribuídos para os dispositivos alvo, clique em **Aprovar imediatamente**. Entretanto, se você quiser avaliar primeito os arquivos de definição de vírus, antes de distribuí-los para os dispositivos gerenciados, clique em **Restringir definições a um test piloto primeiro**. (Você pode também configurar um período de aprovação automático e um período mínimo de teste para evitar ter que fazer isso manualmente após o teste). Se preferir fazer primeiro o teste piloto, os arquivos de definição de vírus serão descarregados em uma pasta de teste piloto para que sejam distribuídos para os dispositivos cujas configurações de antivírus instruem o download da versão "piloto" dos arquivos de definição.
9. Se você quiser que apareça uma mensagem pop-up no console do servidor núcleo quando os arquivos de definição de vírus não for atualizado nos últimos sete dias, clique em **Mostrar diálogo de lembrete se as definições estiverem desatualizadas**.
10. Se desejar fazer download agora dos arquivos de definição mais recentes, clique em **Obter últimas definições**. A caixa de diálogo **Atualização de definições** mostra a operação atual e o status.
11. Se desejar aprovar as definições de vírus que residem atualmente na pasta do teste piloto, clique em **Aprovar agora**. Essa ação transfere os arquivos de definição da pasta de teste piloto para a pasta padrão (\LDLogon\Antivirus\Bases).
12. Se desejar salvar uma cópia de backup dos arquivos de definição de vírus residentes na pasta Bases, selecione a opção **Fazer backups**. Você pode restaurar os backups de arquivos de definição sempre que desejar. Os backups são úteis se desejar reverter para uma versão anterior do arquivo de definição de vírus. (Os backups de arquivo de definições são salvos em pastas separadas nomeadas por data e hora de criação, no diretório \LDLogon\Antivirus\Backups\)
13. Clique em **Descarregar agora** para fazer download das suas atualizações de conteúdo de segurança selecionadas. A caixa de diálogo **Atualização de definições** mostra a operação atual e o status. Ou clique no botão **Agendar download** para cirar uma tarefa agendada (veja abaixo).

14. Quando a atualização estiver concluída, clique em **Fechar**. Observe que se você clicar em **Cancelar** antes do término da atualização, somente o conteúdo de segurança que já foram processadas até este ponto são inseridas no banco de dados núcleo. Seria necessário executar a atualização novamente para obter o conteúdo de segurança restante.

IMPORTANTE: Uma mini-análise nos processos da memória é executada no dispositivo quando os arquivos de definição de vírus são atualizados nos dispositivos gerenciados. Essa análise é feita para assegurar que os processos em execução na memória na hora da atualização ainda estão limpos.

Agendamento de atualizações automáticas de arquivo de definição de vírus

Também é possível configurar as atualizações de arquivo de definição de vírus como tarefas agendadas a serem executadas futuramente ou como uma tarefa recorrente.

Para isso, configure as opções de download de conteúdo de segurança na caixa de diálogo **Atualizar downloads** selecionando as atualizações do LANDesk Antivirus na lista de tipo de definições na guia **Atualizações**. Em seguida, configure as opções de arquivo de definição de vírus na guia **LANDesk Antivirus** e clique no botão **Agendar atualização**. A caixa de diálogo **Informações de atualização agendada** mostra configurações específicas à tarefa. Digite um nome para a tarefa e clique em **OK** para criar uma tarefa de Download de conteúdo de segurança na ferramenta Tarefas agendadas, onde você pode especificar as opções de agendamento.

NOTA: Configurações de tarefas e específicas globais
Observe que somente os tipos de definição, idiomas e configurações de download de definição e patch são salvos e associados a uma tarefa específica ao criá-la. Essas três definições são consideradas específicas a tarefas. Entretanto, todas as definições nas outras páginas da caixa do diálogo **Download de atualizações** são globais, o que significa que se aplicam a todas as tarefas subsequentes de download de conteúdo de segurança. As configurações globais de download do patch, servidor proxy, correção automática de spyware, alertas de segurança e antivírus. Quando você mudar configurações globais, ela estará em efeito para todas as tarefas de download de conteúdo de segurança daquele ponto em diante.

Avaliar arquivos de definição de vírus com um teste piloto

Você pode decidir avaliar os arquivos de definição de vírus antes de distribuí-los para todos os dispositivos gerenciados. Isso pode ser feito facilmente através da restrição das atualizações de arquivo de definição de vírus a uma pasta de teste piloto e, em seguida, aplicar configurações de antivírus selecionando a opção **Fazer download da versão piloto dos arquivos de definição de vírus**.

Para executar um teste piloto de arquivos de definição de vírus

1. Na guia **LANDesk Antivirus** da caixa de diálogo **Fazer download da atualização**, clique em **Limitar primeiramente ao teste piloto**.
2. Se você não quiser mover manualmente os arquivos de definições de vírus testados da pasta de teste piloto para a pasta padrão (\LANDesk\ManagementSuite\ldlogon\antivirus8\win\bases8), clique em **Aprovar agenda** para criar uma tarefa agendada especifique um hora para aprovar os arquivos de teste piloto. Preencha os campos na tarefa, que é exibido na ferramenta Tarefas agendadas. Quando a hora especificada chegar, os arquivos de definição de vírus são aprovados automaticamente e movidos.

3. Para fazer o download dos arquivos mais recentes de definições de vírus do servidor de conteúdo do LANDesk Security Suite, clique em **Obter definições mais recentes**.
4. Para aprovar imediatamente os arquivos de definição de vírus que residem atualmente na pasta do teste piloto, clique em **Aprovar agora**. Isto move os arquivos de definições de vírus da pasta de teste piloto para a pasta padrão (\LANDesk\ManagementSuite\ldlogon\antivirus8\win\bases8).
5. A seguir, crie configurações de teste piloto de antivírus que permita distribuir os arquivos de definição de vírus a um conjunto limitado de computadores de teste. Na página **Atualizações do arquivo de definição de vírus** da configuração de antivírus, selecione **Fazer download da versão piloto dos arquivos de definição**.
6. Aplique as configurações de antivírus de teste piloto a uma tarefa de análise antivírus a qual você pode usar para selecionar como alvo o seu conjunto limitado de computadores de teste. Agora você pode observar a atividade de análise antivírus e os resultados nesses dispositivos a fim de avaliar a eficácia dos arquivos de definição de vírus antes de distribuí-los a um conjunto mais amplo.

Backup de arquivos de definição de vírus

Se desejar salvar versões antigas de arquivos de definição de vírus, use as configurações de **Backups de definições de vírus** na guia **LANDesk Antivirus**.

O backup de arquivos de definição de vírus pode ser muito útil se precisar de um arquivo antigo de definições de vírus para analisar e limpar arquivos específicos infectados ou para restaurar um arquivo de definição de vírus que resolveu um problema em particular.

(Os backups de arquivo de definição são salvos em pastas separadas, nomeadas por data e hora na pasta pai \LDLogon\Antivirus\Backups\

Análise de vírus em dispositivos

Esta seção fornece informações sobre a análise de dispositivos gerenciados para vírus conhecidos e objetos suspeitos.

IMPORTANTE: A análise requer a assinatura apropriada de conteúdo
Lembre-se que para poder procurar um tipo de conteúdo de segurança específico, inclusive vírus, é necessário ter a assinatura de conteúdo correspondente do LANDesk Security Suite. Para obter informações sobre assinaturas de conteúdo, entre em contato com o representante da LANDesk ou visite o site da LANDesk:
LANDesk Home Page

Métodos de verificação

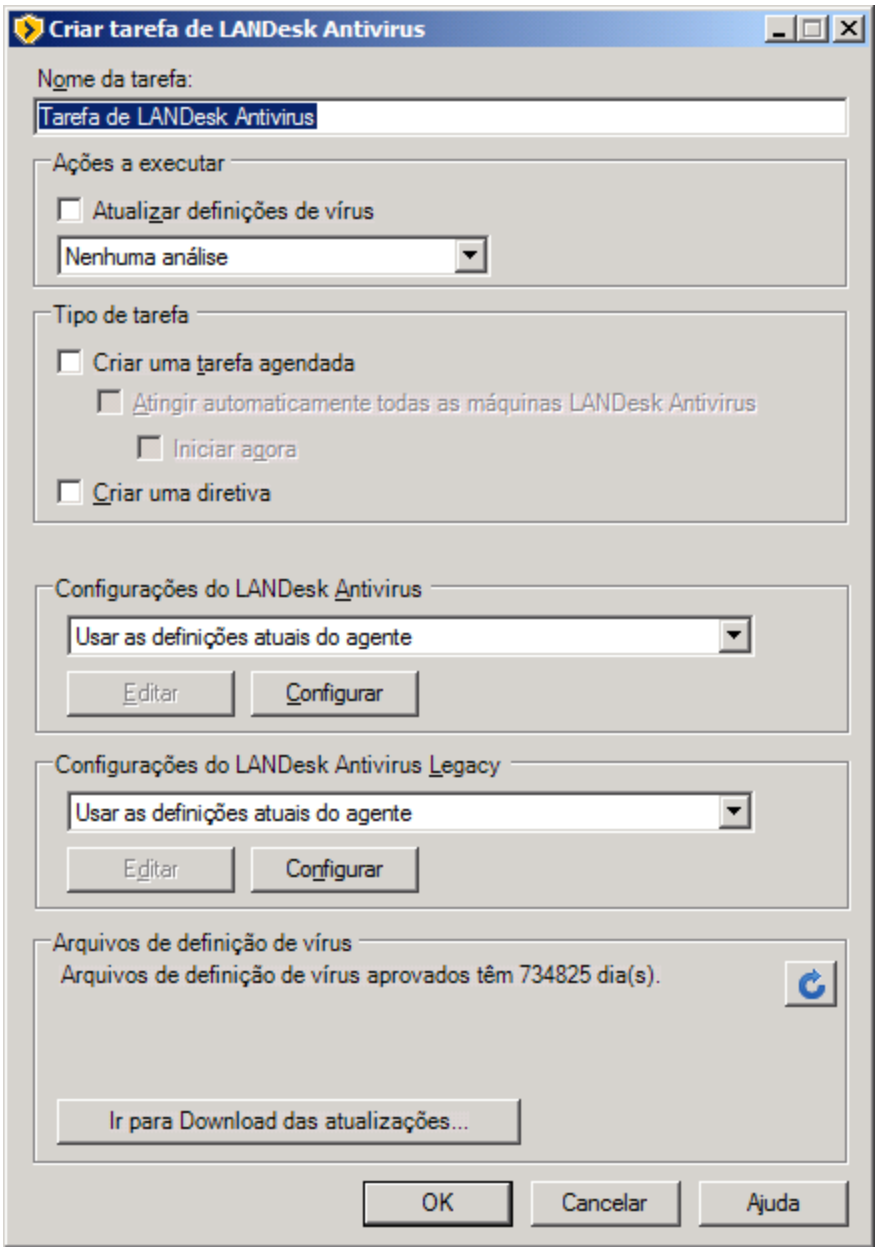
Há vários métodos diferentes de executar uma análise antivírus em dispositivos gerenciados com o Antivirus instalado:

- Análise antivírus agendada
- Análise antivírus por demanda
- Análise antivírus iniciada pelo usuário
- Proteção de arquivos em tempo real
- Proteção de email em tempo real

Executa uma análise antivírus agendada a partir do console

No console, configure tarefas de análise antivírus que podem ser executadas como análise por demanda, tarefa agendada ou diretiva.

A correção de tarefas agendadas pode ser considerada uma distribuição de instalação, pois o patch é instalado do servidor núcleo para os dispositivos, enquanto que uma diretiva é considerada uma distribuição forçada, pois o agente de diretivas nos dispositivos verifica o servidor núcleo quanto às diretivas aplicáveis e então "instala" o patch a partir do servidor núcleo.



Para criar uma tarefa de análise antivírus

1. Clique em **Ferramentas > Segurança > Configurações de segurança**.
2. Certifique-se de que os arquivos de definição de vírus foram atualizados recentemente.
3. Verifique se a pasta do arquivo de definição de vírus (\LDLogon\Antivirus\Bases) contém apenas as definições que você deseja analisar.
4. Clique no botão **Criar uma tarefa** na barra de ferramentas e em **LANDesk Antivirus**.
5. Digite um nome para a tarefa.
6. Especifice se deseja que esta tarefa atualize as definições de vírus, execute a análise de antivírus ou faça as duas.
7. Especifique se a tarefa é uma tarefa agendada ou uma análise baseada em diretivas, ou ambas.
8. Se desejar analisar *todos* os dispositivos com agente LANDesk Antivirus instalado, selecione uma tarefa agendada e em seguida, selecionar todos os dispositivos. Você também pode iniciar imediatamente a análise antivírus de todos os dispositivos.
9. Selecione a opção **Atualizar definições de vírus** se desejar garantir que a análise utilize os arquivos de definição de vírus conhecidos mais recentes.
10. Selecione uma configuração antivírus na lista disponível (ou crie uma configuração personalizada dessa análise clicando no botão **Configurar**) para especificar como a análise funciona nos dispositivos do usuário final. Se desejar que a análise antivírus utilize as configurações antivírus local do dispositivo (configurações padrão), selecione essa opção na lista. Mais informações sobre como configurar a análise antivírus com configurações antivírus são encontradas na caixa de diálogo"Sobre a caixa de diálogo Configurações do LANDesk Antivirus" na página 741.
11. Clique em **OK**. (Para uma análise agendada da tarefa típica, clique em **OK**, adicione dispositivos alvo e configure as opções de agendamento na ferramenta Tarefas agendadas.)

Executa uma análise antivírus por demanda a partir do console

Você pode também executar uma análise antivírus imediata por demanda em um ou mais dispositivos alvo.

Para fazer isso, clique com o botão direito no dispositivo selecionado (ou até 20 dispositivos selecionados em conjunto), clique em **Análise LANDesk Antivirus agora**, selecione definições de antivírus, escolha se deseja uma atualização dos arquivos de definição de vírus antes da análise e, em seguida, clique em **OK**.

Quando você clica em OK, a caixa de diálogo **Status das ações solicitadas** mostra as seguintes informações:

- Andamento
- Resultados
- Informações do tempo de análise

Executa uma análise antivírus no dispositivo gerenciado

Além disso, se você tiver definido as configurações antivírus para mostrarem o ícone do Antivirus na bandeja do sistema do dispositivo, os usuários finais podem executar suas próprias análises antivírus por demanda.

Para fazer isso no dispositivo gerenciado, clique com o botão direito na barra de tarefas do **LANDesk Antivirus** e selecione **Analisar meu computador**. Ou, na caixa de diálogo Antivirus, clique em **Analisar meu computador**.

Habilitar a proteção antivírus em tempo real (arquivo, e-mail)

A proteção antivírus em tempo real fornece análises contínuas no plano de fundo de arquivos específicos, tipos de arquivos, mensagens de email e anexos de email com base em definições de vírus conhecidos. Você pode também habilitar a notificação em tempo real para informar os usuários finais sobre arquivos infectados.

A proteção em tempo real, análise de email e notificação são configuradas com parâmetros antivírus.

NOTA: Indicador do ícone do LANDesk Antivirus na bandeja do sistema
Quando a proteção antivírus em tempo real está ativada, o ícone do LANDesk Antivirus na bandeja do sistema (no dispositivo do usuário final) fica amarelo. Quando a proteção em tempo real está desativada o ícone permanece esmaecido.

Proteção de arquivos em tempo real

Configure a proteção de arquivo em tempo real com as opções da página **Proteção em tempo real** da caixa de diálogo **Definições de antivírus**. Para obter mais informações, clique em **Ajuda**.

Quando a proteção em tempo real está em execução, os arquivos são analisados para detectar vírus toda vez que são:

- Abertos
- Fechados
- Acessados
- Copiados
- Salvos

Análise de email em tempo real

Configurar a Análise de e-mail em tempo real na opção **Habilitar análise de e-mail** na página **Geral** da caixa de diálogo **Configurações de antivírus**.

A proteção de email em tempo real fornece análise contínua de mensagens recebidas e enviadas. O Antivírus analisa o corpo da mensagem assim como o corpo de mensagens anexas e os arquivo anexos.

A proteção de email em tempo real do Antivirus suporta:

- Microsoft Outlook

Quando a proteção de email em tempo real está em execução as mensagens e os anexos:

- São analisados quando abertos ou verificados na janela de pré-visualização
- Não são analisados quando selecionados

Quando é descoberto um email infectado em um dispositivo gerenciado, o Antivirus tenta limpá-lo. Se puder se limpo, um novo cabeçalho é colocado no corpo da mensagem para informar o usuário final. Se o e-mail infectado não pode ser limpo, o corpo inteiro da mensagem é excluído e substituído por um novo cabeçalho.

Quando é descoberta uma mensagem de email suspeita, o corpo da mensagem é convertido em texto puro e um cabeçalho é adicionado à mensagem.

Além disso, uma caixa de diálogo é exibida no dispositivo do usuário final que mostra:

- o caminho do arquivo
- o nome do arquivo
- o nome do vírus
- Uma nota solicitando ao usuário final para contatar o administrador da rede

Notificação em tempo real (arquivo infectado)

Usuários finais podem ser notificados quando um arquivo infectado por vírus é detectado, colocado em quarentena, excluído, pulado ou limpo.

Configure a notificação de arquivo infectado em tempo real com a opção da página **Proteção em tempo real** da caixa de diálogo **Definições de antivírus**.

Uma caixa de diálogo é exibida no dispositivo do usuário final que mostra:

- o caminho do arquivo
- o nome do arquivo
- o nome do vírus
- uma nota solicitando ao usuário final para contatar o administrador da rede

Configuração das opções de análise de vírus com as configurações do antivírus

O Antivírus lhe oferece o controle total sobre como as análises de antivírus são executadas nos dispositivos alvo e quais opções estão disponíveis aos usuários finais. Por exemplo, dependendo do objetivo ou do tempo agendado de uma análise antivírus, pode ser útil exibir o cliente do Antivírus nos dispositivos dos usuários finais, permitir ao usuário final executar análises, exibir e restaurar objetos em quarentena, fazer o download das atualizações do arquivo de definição de vírus por si mesmos e assim por diante. Para fazer isso, crie e aplique as configurações antivírus à tarefa de análise.

Com as definições de antivírus você pode configurar as seguintes opções:

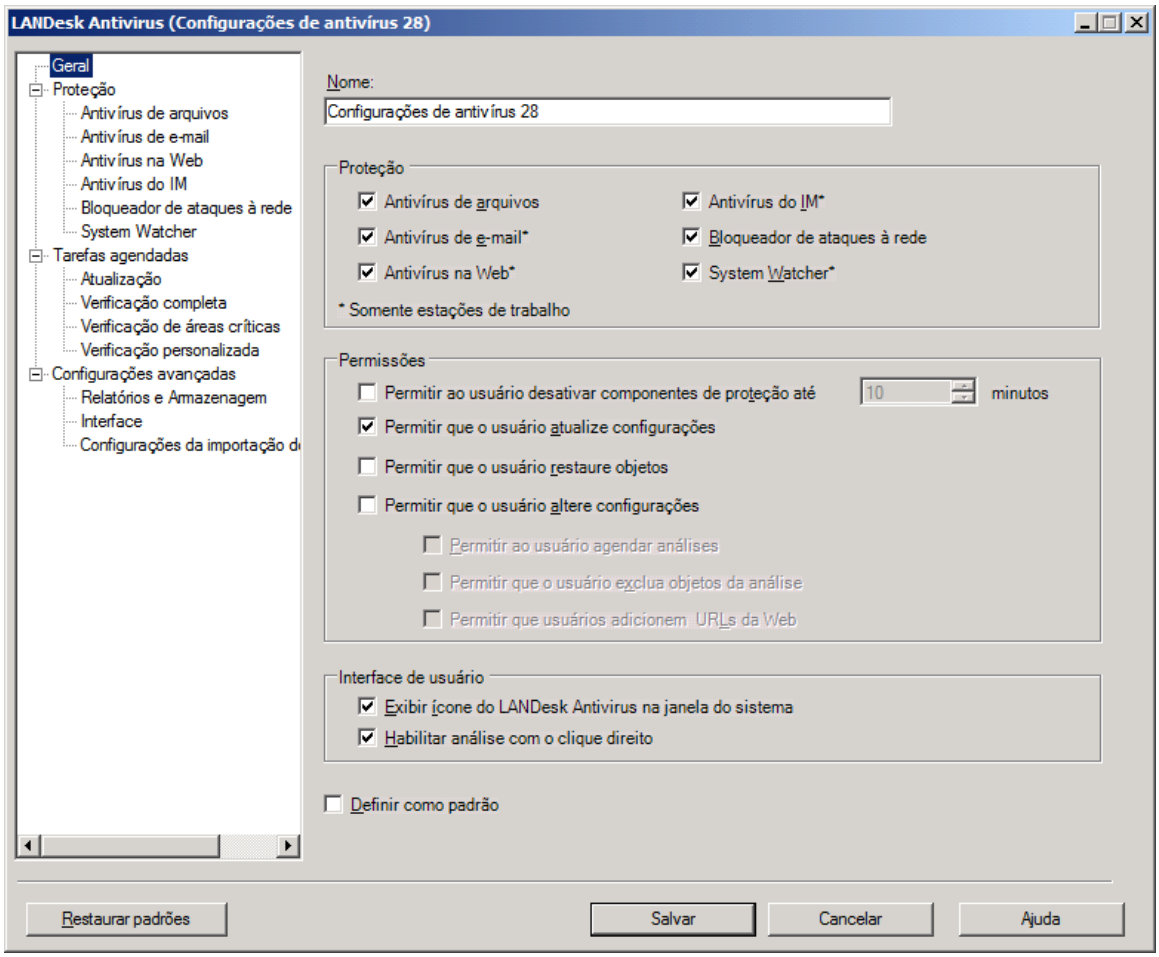
- Se o ícone do Antivirus for exibido nas bandejas de sistema dos dispositivos (desde que o usuário acesse a análise antivírus, a tela de quarentena e backup e as tarefas de manipulação de arquivo)
- Análise de email em tempo real
- Análises com um clique do botão direito do mouse do usuário final
- Uso da CPU
- Proprietário (para restringir o acesso)
- Análises antivírus agendadas
- Tamanho da pasta de quarentena/backup
- Restauração de objetos infectados e suspeitos
- Quais arquivos, pastas e tipos de arquivo analisar
- Exclusões de análise
- Uso ou não de análise heurística para detectar arquivos suspeitos
- Analisar ou não para detecção de riskware
- Proteção de arquivos em tempo real (inclusive a decisão sobre quais arquivos analisar, heurística e exclusões)

- Download de atualizações de arquivos de definição de vírus (versões de teste piloto, downloads agendados, permissão de download aos usuários finais e downloads diretos do servidor de conteúdo de segurança)

Todas as definições de antivírus que você cria são armazenadas no grupo **LANDesk Antivirus** localizado na ferramenta **Configurações de segurança**.

Uso das configurações de Antivirus:

Criar e aplicar definições de antivírus (um conjunto salvo de opções configuradas) às tarefas de análise antivírus. Você pode criar quantas definições antivírus desejar. As definições de antivírus podem ser criadas para um fim, tempo ou conjunto de dispositivos alvo específicos.



Para criar definições de antivírus

1. Na ferramenta **Configurações de segurança**, clique com o botão direito no objeto **LANDesk Antivirus** e, em seguida, clique em **Novo**. (Nota: Você pode também acessar esta caixa de diálogo clicando em **Editar** ou **Configurar** em qualquer caixa de diálogo de tarefas onde puder aplicar as definições de antivírus.
2. Digite um nome para as definições de antivírus.
3. Especifique as configurações nas páginas como desejado para a tarefa em particular. Clique em **Ajuda** para obter mais informações sobre uma opção.

Quando configuradas, você poderá aplicar as definições de antivírus às tarefas de antivírus (ou para mudar a tarefa de definições).

Mudança das definições de antivírus padrão de um dispositivo

As definições de antivírus padrão de um dispositivo são distribuídas como parte da configuração inicial do agente. Quando uma tarefa específica tem definições diferentes de antivírus associadas ou a ela atribuídas, as definições padrão são canceladas. Se preferir, você pode usar as configurações padrão selecionando-a quando criar a tarefa.

Para determinados dispositivos, porém, você pode decidir mudar essas definições de antivírus padrão. O Patch e Conformidade fornece um meio de fazer isso sem ter que redistribuir uma configuração nova e completa. Para fazer isso, use a tarefa **Mudar configurações** localizada na lista suspensa do botão **Criar uma tarefa**. A caixa de diálogo que é exibida permite digitar um nome exclusivo para a tarefa, especificar se se trata de uma tarefa agendada ou de uma diretiva e selecionar definições de antivírus existentes como padrão ou usar o botão Editar para criar novas definições de antivírus como padrão para os dispositivos alvo.

Exibição das configurações de antivírus de um dispositivo no Inventário

Você pode descobrir e/ou verificar as configurações de antivírus de um dispositivo em sua tela Inventário.

Para fazer isso, clique com o botão direito do mouse no dispositivo e clique em **Inventário > LANDesk Management > Configurações do AV**.

Configuração dos arquivos a serem analisados (arquivos infectáveis somente, exclusões, heurística, riskware)

Você pode especificar os arquivos (itens) que deseja analisar e quais arquivos você não deseja analisar com as análises de antivírus e a proteção antivírus de arquivos em tempo real.

Consulte as seguintes seções para obter informações sobre a personalização dos itens que serão analisados:

- "Todos os arquivos ou somente os arquivos infectáveis" na página 729
- "Exclusão de itens das análises de antivírus e da proteção em tempo real" na página 731
- "Uso de análise heurística para detectar objetos suspeitos" na página 731
- "Análise de riskware (banco de dados estendido)" na página 732

Todos os arquivos ou somente os arquivos infectáveis

Você pode analisar todos os arquivos ou apenas os arquivos infectados nas páginas **Análise de vírus** e **Proteção em tempo real** de definições de antivírus.

- **Analisar todos os tipos de arquivos:** Especifica que os arquivos de todos os tipos no dispositivo alvo são analisados por uma análise antivírus. Como isso pode levar bastante tempo, é aconselhado analisar todos os tipos de arquivos em uma análise em demanda em vez de proteção em tempo real.
- **Só analisar arquivos infectáveis:** Especifica que somente os arquivos infectáveis são analisados. Arquivos infectáveis são de tipo vulneráveis a infecções de vírus. Analisar somente os arquivos infectáveis é mais eficiente do que analisar todos os arquivos porque alguns vírus afetam somente certos tipos de arquivos. No entanto, certifique-se de verificar regularmente todos os arquivos com um análise por demanda para garantir que os dispositivos permaneçam limpos.

Tipos de arquivos infectáveis

Os tipos de arquivos infectáveis são determinados por seus identificadores de formato no cabeçalho de cada arquivo, e não pela extensão do arquivo, para garantir que os arquivos renomeados sejam analisados.

Os arquivos infectáveis incluem: arquivos de documentos como Word e Excel; arquivos modelo associados a arquivos de documento e arquivos de programa como dynamic link libraries (.DLLs), arquivos de comunicação (.COM), arquivos executáveis (.EXEs) e outros arquivos de programa. Veja abaixo uma lista dos tipos de arquivos infectáveis pela extensão padrão ou original do formato do arquivo.

- ACM
- ACV
- ADT
- AX
- BAT
- BIN
- BTM
- CLA
- COM
- CPL
- CSC
- CSH
- DLL
- DOC
- DOT
- DRV
- EXE
- HLP
- HTA
- HTM
- HTML
- HTT
- INF
- INI
- JS
- JSE
- JTD
- MDB
- MSO
- OBD
- OBT
- OCX
- PIF

- PL
- PM
- POT
- PPS
- PPT
- RTF
- SCR
- SH
- SHB
- SHS
- SMM
- SYS
- VBE
- VBS
- VSD
- VSS
- VST
- VXD
- WSF
- WSH

Exclusão de itens das análises de antivírus e da proteção em tempo real

Também é possível especificar quais arquivos você não deseja analisar com as análises antivírus e com a proteção de arquivo em tempo real. Configure exclusões de análise antivírus adicionando arquivos, pastas e tipos de arquivos à lista de exclusão nas páginas de configuração de antivírus **Análise de vírus** e **Proteção em tempo**.

NOTA: Lista de itens confiáveis nos dispositivos gerenciados
Observe que você também pode habilitar uma opção permitindo os usuários finais a especificar arquivos e pastas que não devem ser analisados pelo LANDesk Antivirus. Este recurso é chamado lista de itens confiáveis e é configurado na página **Geral** das configurações do antivírus.

Uso de análise heurística para detectar objetos suspeitos

Você pode habilitar a análise heurística para detectar arquivos suspeitos (possivelmente infectados) com as análises antivírus e a proteção de arquivo em tempo real.

Habilite a análise heurística nas páginas de configurações de antivírus **Análise de vírus** e **Proteção em tempo real**.

A análise heurística tenta detectar arquivos suspeitos de infecção de vírus (não definidos no banco de dados de assinaturas de vírus) considerando o comportamento suspeito do arquivo. O comportamento suspeito pode ser um programa que está se modificando a si mesmo, que tenta encontrar outros executáveis imediatamente ou que é modificado após ser fechado. A análise heurística emula a execução do programa para criar protocolos de atividades suspeitas observadas e utiliza esses protocolos para identificar as possíveis infecções de vírus. Em quase todos os casos, esse mecanismo é eficaz e confiável e raramente produz falsos positivos.

O Antivirus utiliza um analisador heurístico para verificar arquivos que já foram analisados por antivírus com base nas definições conhecidas.

Observe que a análise heurística pode afetar negativamente o desempenho em dispositivos gerenciados.

Análise de riskware (banco de dados estendido)

O Antivirus permite a habilitação de software de risco, também conhecido como riskware, nos dispositivos alvo. Software de risco é software cliente cuja instalação apresenta uma possibilidade de risco embora não seja definitiva, ao usuário final.

Exemplos de riskware incluem adware, programas proxy, pornware, utilitários remotos de administração, IRC, discadores, monitores de atividade, utilitários de senha e ferramentas da Internet, como, por exemplo FTP, Web, Proxy e Telnet.

Ao selecionar uma análise de dispositivos gerenciados para verificar software de risco, o Antivirus carrega um banco de dados estendido com arquivos de definição usados para realizar a análise. A análise do banco de dados estendido é mais demorada do que a análise padrão de antivírus.

Observações adicionais sobre análise de arquivos

- **Análise do ponto de restauração do sistema:** Antivirus analisará os arquivos em quaisquer pastas de ponto de restauração de sistema que possam existir no dispositivo gerenciado.

O que acontece com o dispositivo durante a análise de vírus

Esta seção descreve como o Antivirus é exibido em dispositivos do usuário final com o antivírus instalado e o que acontece quando os dispositivos são verificados em busca de vírus por uma análise antivírus ou pela proteção contra vírus em tempo real. As opções de usuário final são listadas, assim como as ações que os usuários finais podem executar quando um objeto infectado é descoberto pela análise.

Interface do cliente do Antivirus e ações do usuário final

Se a opção **Mostrar ícone do LANDesk Antivirus na bandeja do sistema** estiver selecionada nas definições de antivírus do dispositivo, o cliente Antivirus será aberto e mostrará os seguintes elementos:

Ícone da bandeja do sistema

- Proteção em tempo real é ativada (o ícone da bandeja do sistema é amarelo) ou desativada (o ícone da bandeja do sistema está esmaecido)

Janela do Antivirus

- A proteção em tempo real é ativada ou desativada (se a opção estiver ativada nas configurações de antivírus, o usuário final poderá desativar a proteção em tempo real pelo período que você especificar)
- Análise de e-mail é ativada ou desativada
- Análise mais recente (data e hora)

- Análise agendada (data e hora)
- Número da versão do mecanismo de análise
- Definições de vírus (a última vez em que os arquivos padrão foram atualizados)
- Quarentena (exibe o número de objetos em quarentena. Os usuários finais precisam clicar em **Exibir detalhes** para acessar a caixa de diálogo Objetos em quarentena. Se a opção estiver habilitada, o usuário final pode também restaurar arquivos. Se a opção de requisito de senha estiver habilitada, o usuário final deve inserir a senha.)
- Backup (mostra o número de objetos em backup)
- Itens confiáveis (mostra os itens adicionados pelo usuário final à lista de itens confiáveis que não serão analisados a procura de vírus ou software de risco)

Ações do usuário final

Se o Antivirus estiver instalado no computador, e suas definições de antivírus (padrão ou específico a tarefa) permitirem, os usuários podem executar as seguintes tarefas:

- Analisar o computador (exibir o status, pausar e cancelar a análise)
- Clicar com o botão direito para fazer análise antivírus nos arquivos e nas pastas do Windows Explorer (se a opção estiver habilitada pela configuração do antivírus)
- Exibir as tarefas de análise antivírus agendadas locais
- Criar análises antivírus agendadas locais no computador (se a opção estiver habilitada pela configuração do antivírus)
- Atualizar arquivos de definição de vírus
- Desabilitar temporariamente a proteção em tempo real (se a opção for habilitada pela configuração do agente e limitada a um período de tempo especificado)
- Exibir objetos em quarentena
- Exibir objetos de backup
- Exibir itens confiáveis
- Restaurar objetos suspeitos (se a opção for habilitada pela configuração de antivírus)
- Restaurar objetos infectados e software de risco (se a opção estiver habilitada pela configuração do antivírus)
- Adicionar e remover arquivos e pastas/subpastas da lista de itens confiáveis

Observe que os usuários finais não podem configurar análises de antivírus ou desabilitar análise de e-mail.

Quando um objeto infectado é detectado

Este processo aplica-se a arquivos e mensagens de e-mail infectados.

1. O backup do objeto infeccionado é feito automaticamente. (O arquivo de backup é salvo na pasta \LDClient\Antivirus\, com uma extensão *.bak.)
2. É feita uma tentativa de limpar o objeto infectado.
3. Se o objeto infectado puder ser limpo, ele será restaurado ao seu local original.
4. Se o objeto infectado não puder ser limpo, ele será colocado em quarentena. (A string de vírus é removida e o arquivo é criptografado para não ser executado. O arquivo em quarentena é salvo na pasta \LDClient\Antivirus\, com uma extensão *.qar.)

Se a opção correspondente estiver habilitada em suas definições de antivírus (padrão ou específica à tarefa), os usuários finais poderão restaurar, excluir e analisar novamente os objetos em quarentena.

Análise automática de arquivos em quarentena

Quando uma análise antivírus por demanda é executada ou quando os arquivos de definição de vírus são atualizados, o analisador antivírus verifica automaticamente os objetos na pasta de quarentena para ver se algum dos arquivos infectados podem ser limpos com os arquivos de definição atuais de vírus.

Se um arquivo em quarentena puder ser limpo, ele é restaurado automaticamente e o usuário é notificado.

Os usuários finais podem abrir um arquivo de backup para ver o cabeçalho que fornece informações sobre o local do arquivo original e o motivo do backup.

Observe que apenas o usuário original (o usuário que fez o logon quando o arquivo infectado foi descoberto) tem permissão para excluir ou modificar arquivos de backup.

Configurar alertas de antivírus

Você pode configurar alertas de antivírus de forma a ser notificado quando forem detectados infecções de específicas de antivírus em dispositivos gerenciados no seu sistema. O Antivirus usa a ferramenta padrão de alerta da LANDesk.

Você define os parâmetros da infecção de vírus com base no número de dispositivos gerenciados infectados por um vírus em um período especificado.

Para configurar alertas de antivírus

As definições de alerta de antivírus são encontradas na guia **Antivírus** da caixa de diálogo **Configurações de alerta**.

É necessário primeiro configurar os alertas de antivírus na ferramenta Configurações de alerta no console. Os alertas de antivírus incluem:

- Falha em uma ação de alerta do antivírus
- Êxito em uma ação de alerta do antivírus
- Alerta de ataques de vírus (por vírus)

Os seguintes eventos de antivírus podem gerar alertas de antivírus:

- A remoção do vírus falhou
- A remoção do vírus teve êxito
- A quarentena falhou
- A quarentena teve êxito
- A exclusão falhou
- A exclusão teve êxito

Selecione os alertas que desejar gerar. A opção de intervalo permite impedir a ocorrência de alertas em demasia. Se houver mais de um alerta (para qualquer disparo de antivírus) durante um intervalo especificado, ele será ignorado.

É possível exibir o histórico completo do alerta de antivírus de um dispositivo no modo de exibição Informações de segurança. Clique com botão direito no dispositivo, selecione Informações de segurança, selecione o tipo de Antivírus na lista suspensa Tipo e, a seguir, selecione o objeto Histórico de antivírus.

Gerar relatórios de antivírus

Informações de antivírus são representadas por vários relatórios na ferramenta Relatórios. Esses relatórios fornecem informações úteis sobre a atividade análise e status de antivírus para dispositivos analisados na sua rede.

Para acessar a ferramenta Relatórios e gerar e exibir relatórios, o usuário precisa ter permissões de administrador LANDesk (o que implica permissões totais) ou as permissões específicas para a função Relatórios.

Para obter mais informações sobre o uso da ferramenta Relatórios, consulte "Relatórios" na página 197.

Exibição de informações de antivírus no Dashboard executivo

Você também pode exibir informações de análise do antivírus no Executive Dashboard do console Web da LANDesk. Esses dados são úteis para identificar ataques de vírus e para mostrar a proteção antivírus em função do tempo decorrido.

Os componentes específicos ao LANDesk Antivirus mostram:

- Os cinco vírus mais importantes detectados (nos últimos 10 dias ou semanas)
- Os dispositivos gerenciados infectados com vírus (nos últimos 10 dias ou semanas)
- Porcentagem de dispositivos gerenciados com a proteção em tempo real ativada
- Porcentagem de dispositivos gerenciados com definições de vírus atualizadas

Ajuda do LANDesk Antivirus

As características do LANDesk Antivirus são acessadas pela janela da ferramenta Configurações de agente (**Ferramentas > Segurança e conformidade > Configurações de agente**).

O Antivirus permite o download e o gerenciamento do conteúdo de antivírus (arquivos de definição de vírus), a configuração de análises de antivírus, a personalização das definições de tela/interação do analisador de antivírus que determinam a maneira do analisador ser exibido e funcionar nos dispositivos alvo e quais opções interativas são disponíveis aos usuários finais. Você também pode ver informações para os dispositivos analisados, habilitar alertas e gerar relatórios de antivírus.

A seção principal do "LANDesk Antivirus" na página 712 introduz esta ferramenta de gerenciamento de segurança de segurança, o qual é um componente de LANDesk Management Suite e LANDesk Security Suite. Esta seção contém uma visão geral, informações de assinatura do conteúdo de antivírus e instruções detalhadas sobre como usar os recursos do LANDesk Antivirus.

Essa seção contém os seguintes tópicos de ajuda que descreve as mensagens do Antivirus. Pela interface do console, esses tópicos de ajuda são acessados clicando no botão **Ajuda** em suas respectivas caixas de diálogo.

- "Ajuda do Download de atualizações de antivírus" na página 736
- "Ajuda das tarefas do antivírus" na página 739
- "Ajuda de configurações antivírus" na página 741

Ajuda do Download de atualizações de antivírus

Sobre a página LANDesk Antivirus na caixa de diálogo Download das atualizações

Use a página **LANDesk Antivirus** na caixa de diálogo **Download de atualizações** para configurar definições para o download das atualizações de arquivo de definição de vírus nos serviços LANDesk Security Suite. Você pode selecionar o download do conteúdo do Antivirus (arquivos de definição/padrões de vírus), especificar o horário da disponibilização dos arquivos de definição de vírus para distribuição aos dispositivos gerenciados (imediatamente ou após o período de teste piloto) e se os arquivos de definição terão backup.

É importante notar que a página **Atualizações** da caixa de diálogo **Download de atualizações** inclui várias atualizações antivírus na lista de tipos de definições, inclusive uma denominada Atualizações LANDesk Antivirus. Quando você seleciona este tipo o conteúdo de detecção do analisador E as atualizações do arquivo de definições de vírus descarregados.

Atualizações de antivírus são definições de análise que detectam:

- instalação de mecanismos de análise antivírus comuns (incluindo o agente LANDesk Antivirus)
- status de análise em tempo real (ativado ou desativado)
- versões do arquivo de padrões específicos do analisador (atualizado ou antigo)
- data da última análise (se a análise mais recente estiver dentro do período máximo permitido especificado pelo administrador)

NOTA: Conteúdo de detecção do analisador de antivírus comparado com o conteúdo de definições
As atualizações de antivírus não implicam na existência de arquivos de definição (ou padrões) de vírus. Quando você faz o download das atualizações antivírus de terceiros, apenas o conteúdo de detecção do analisador é baixado para o repositório padrão, mas não os arquivos de definição de vírus específicos do analisador. Quando você faz o download das Atualizações LANDesk Antivirus, o conteúdo de detecção do analisador E as atualizações do arquivo de definições de vírus do LANDesk Antivirus são baixados. Os arquivos de definição de vírus do LANDesk Antivirus são baixados em um local separado no servidor núcleo. O repositório padrão do arquivo de definições de vírus é a pasta \LDLogon\Antivirus\Bases.

Você deve ter a assinatura de conteúdo LANDesk Security Suite correta para fazer o download de cada tipo de conteúdo de segurança.

Uma instalação básica do LANDesk Management Suite permite o download e a análise de atualizações de software LANDesk e a criação e uso das suas definições personalizadas. Para todos os outros tipos de conteúdo de segurança e patch, como vulnerabilidades específicas de plataforma, spyware e a inclusão de arquivos de definição de vírus (padrão), você DEVE ter uma assinatura de conteúdo do LANDesk Security Suite para fazer o download das definições correspondentes.

Para obter mais informações sobre as assinaturas de conteúdo do Security Suite, contate seu revendedor ou visite o site da LANDesk.

LANDesk Home Page

Após especificar os tipos de conteúdo que deseja fazer download e as outras opções na caixa de diálogo Fazer o download das atualizações:

- Para fazer um download imediato, clique em **Atualizar agora**. Se você clicar em **Aplicar**, as configurações especificadas serão salvas e exibidas na próxima vez em que você abrir essa caixa de diálogo. Você deverá confirmar se deseja salvar as configurações ao clicar em **Fechar**.
- Para agendar uma tarefa de download de conteúdo de segurança, clique em **Agendar atualização** para abrir a caixa de diálogo **Informações de atualização agendada**, digite um nome para a tarefa, verifique as informações da tarefa e clique em **OK** para adicionar a tarefa às Tarefas agendadas.

IMPORTANTE: Configurações de tarefas e específicas globais
Observe que somente os tipos de definição, idiomas e configurações de download de definição e patch são salvos e associados a uma tarefa específica ao criá-la. Essas três definições são consideradas específicas a tarefas. Entretanto, todas as definições nas outras páginas da caixa de diálogo **Download de atualizações** são globais, o que significa que se aplicam a todas as tarefas subseqüentes de download de conteúdo de segurança. As configurações globais de download do patch, servidor proxy, correção automática de spyware, alertas de segurança e antivírus. Quando você mudar configurações globais, ela estará em efeito para todas as tarefas de download de conteúdo de segurança daquele ponto em diante.

Para salvar as mudanças em qualquer página dessa caixa de diálogo a qualquer hora, clique em **Aplicar**.

A página **LANDesk Antivirus** contém as seguintes opções:

- **Definições de vírus aprovadas para distribuição:** Mostra a data e o número de versão dos arquivos de definição de vírus aprovados mais recentemente e que estão agora disponíveis para distribuição aos dispositivos gerenciados. Os arquivos aprovados de definição de vírus se encontram na pasta padrão (\LDLogon\Antivirus\Bases) a partir da qual são distribuídos aos dispositivos alvo como parte das análises de antivírus agendadas e em demanda. A hora exata da atualização do arquivo de definição de vírus (faça o download no serviço da Web do LANDesk Security Suite, que contém os últimos arquivos padrão conhecidos) é exibida em parênteses abaixo desse campo.
- **Definições de vírus em teste piloto no momento:** Observe que esta lista é exibida apenas se você selecionar **Limitar a primeira opção do teste piloto**. Mostra a data e o número da versão dos arquivos de definição de vírus atualmente na sua pasta piloto, se você tiver feito o download das definições de vírus a esse local. O teste piloto o ajuda a verificar a validade e utilidade de um arquivo de definição de vírus antes de usá-lo para analisar os seus dispositivos gerenciados contra vírus. Definições de vírus descarregadas na pasta de teste piloto podem ser distribuídas a dispositivos alvo designados como "teste".

- **Atualizações das definições de vírus - Quando novos arquivos de definições de vírus são baixados da LANDesk:**
  - **Aprovar imediatamente (fazê-las disponíveis a todos os computadores):** Fazer o download de definições de vírus diretamente da pasta padrão (\LANDesk\ManagementSuite\ldlogon\antivirus8\win\bases8). As definições de vírus descarregadas na pasta padrão são aprovadas e podem ser distribuídas aos dispositivos alvo para análise antivírus.
  - **Limitar primeiramente ao teste piloto:** Descarrega arquivos de definição de vírus na pasta piloto para teste. Definições de vírus na pasta piloto podem ser distribuídas a máquinas de teste antes da distribuição aos seus dispositivos gerenciados.
    - **Obter últimas definições:** Inicia um processo imediato de descarregamento no arquivo de definição de vírus. A caixa de diálogo **Atualização de definições** mostra o progresso do download.
    - **Aprovar agora:** Permite mover os arquivos de definição de vírus da pasta piloto à pasta padrão e serem distribuídos aos dispositivos alvo para análise antivírus.
    - **Agendar a aprovação:** Abre a ferramenta Tarefas agendadas com uma nova tarefa que você pode especificar nas opções de agendamento (iniciar agora ou iniciar em uma data e hora específica, e definir a recorrência). Esta tarefa agendada move os arquivos de definições de vírus automaticamente da pasta de teste piloto para a pasta padrão (\LANDesk\ManagementSuite\ldlogon\antivirus8\win\bases8). (**NOTA:** Esta opção só é disponível se você estiver limitando as atualizações dos arquivos de definição de vírus a um teste piloto e permite a aprovação dos arquivos de definição. Se você não ativar essa opção, os arquivos de definição de vírus na pasta piloto devem ser aprovados manualmente com o botão **Aprovar agora**.)
- **Backups das definições de vírus:**
  - **Fazer backups de definições anteriores:** Salva os descarregamentos de arquivos anteriores de definição de vírus. Isso pode ser útil se precisar de um arquivo antigo de definição para analisar e limpar arquivos infectados ou para restaurar um arquivo que resolveu um problema em particular. (Os backups de arquivo de definições são salvos em pastas separadas nomeadas por data e hora de criação, no diretório: \LDLogon\Antivirus\Backups\)
  - **Números de backups a serem mantidos:** Especifica o número de descarregamentos de arquivos de definição de vírus a serem salvos.
  - **História:** Mostra todos os backups disponíveis de arquivos de definição de vírus.
  - **Restaurar:** Move o backup selecionado do arquivo de definição de vírus à pasta padrão de antivírus para que possam ser distribuídos aos dispositivos alvo.
  - **Excluir:** Remove permanentemente o backup selecionado dos arquivos de definição de vírus do servidor núcleo.
- **Descarregar agora:** Faz o descarregamento imediato dos tipos selecionados de conteúdo de segurança. A caixa de diálogo **Atualização de definições** mostra o progresso e o status do descarregamento.

- **Agendar o download:** Abre a caixa de diálogo **Informações de download agendado**, onde você pode digitar um nome único para essa tarefa de download, verificar os downloads e clicar em OK para salvar a tarefa na ferramenta Tarefa agendada. (Observe que somente os tipos de definição, idiomas e configurações de download de definição e patch são salvos e associados quando você cria uma tarefa particular. As configurações de download nas outras páginas desta caixa de diálogo, como local de download de patch, configurações de proxy e configurações de alertas, são globais, o que significa que elas se aplicam a todas as tarefas de download de conteúdo de segurança. Entretanto, você pode mudar essas configurações a qualquer momento e elas estarão em vigor para todas as tarefas de download de conteúdo de segurança desse ponto em diante.)
- **Ver log:** Permite selecionar o local e o nível de detalhes em um arquivo contendo informações de download de definição de vírus.
- **Aplicar:** Salva as suas definições selecionadas de descarregamento para que sejam aplicadas à caixa de diálogo **Download de atualizações** e apareçam na próxima vez em que a caixa de diálogo for aberta.
- **Fechar:** Fecha a caixa de diálogo sem salvar as suas últimas mudanças de configuração.

Para uma descrição das opções nas outras páginas da caixa de diálogo **Download de atualizações**, consulte "Sobre as caixas de diálogo Download das atualizações" na página 621.

Ajuda das tarefas do antivírus

Sobre a caixa de diálogo Criação de tarefa de LANDesk Antivirus

Use esta caixa de diálogo para criar uma tarefa que atualiza os arquivos de definição de vírus, configura análises antivírus em dispositivos alvo (com configurações antivírus) ou para executar essas duas tarefas. As configurações de antivírus derterminam o comportamento do analisador, objetos analisados e as opções do usuário final.

NOTA: Análises de antivírus por demanda
Você pode também executar uma tarefa de antivírus por demanda em um dispositivo através de um menu de atalho de dispositivo.

Esta caixa de diálogo contém as seguintes opções:

- **Nome da tarefa:** identifica a tarefa de análise antivírus com um nome exclusivo.
- **Ações a executar:** Especifica que a tarefa vai fazer. Você pode selecionar uma ou as duas ações.
  - **Atualizações das definições de vírus:** Especifica que a tarefa atualizará os arquivos de definição de vírus baseados nas configurações na página de antivírus da caixa de diálogo Download de atualizações.
  - **Iniciar análise de inventário:** Especifica a hora em que a análise é executada nos dispositivos alvo.

- **Criar uma tarefa agendada:** Adiciona a tarefa de análise à janela de Tarefas agendadas, onde você pode configurar as suas opções de agendamento e recorrência e designar dispositivos alvo.
    - **Tornar alvo todos os computadores LANDesk Antivirus automaticamente:** Adiciona dispositivos gerenciados que foram configurados com o agente do LANDesk Antivirus à lista de dispositivos alvo da tarefa.
    - **Iniciar agora:** Executa a análise antivírus nos dispositivos com o agente do LANDesk Antivirus, adicionando-o à ferramenta de Tarefas agendadas assim que você clicar em **OK**.
    - **Atualizar definições de vírus (inclusive piloto) no núcleo:** Atualiza automaticamente os arquivos padrão de vírus antes que a análise seja iniciada, inclusive arquivos de definição de vírus que residem na pasta piloto. (Nota: A opção Atualizar definições vírus acima precisa ser selecionada para poder usar esta opção.)
- **Criar uma diretiva:** Adiciona uma tarefa de análise antivírus à janela de Tarefas agendadas, onde você pode configurar as opções da diretiva.
- **Definições do LANDesk Antivirus:** Especifica as configurações de antivírus usadas para as tarefas de análise. Configurações de antivírus determinam se o ícone LANDesk Antivirus aparece na bandeja do sistema do dispositivo, disponibilidade de opções interativas para usuários finais, verificação de email e ativação de proteção em tempo real, tipos de arquivos para verificar, arquivos e pastas para excluir, quarentena de arquivo infectado e Backup, verificação agendada de antivírus, e definições de atualizações de vírus agendados. Selecione uma das definições na lista suspensa. Clique em **Editar** para modificar as opções das definições selecionadas. Clique em **Configurar** para criar novas definições.
- **Arquivos de definições de vírus:** Mostra as informações sobre os arquivos de definição descarregados atualmente. Clique em **Download de atualizações** para ir para a página LANDesk Antivirus do Download de atualizações para configurar e agendar um download de arquivo de definição.

Sobre a caixa de diálogo Tarefa de análise LANDesk Antivirus agora

Use esta caixa de diálogo para executar uma análise antivírus imediata por demanda em um ou mais dispositivos alvo.

1. Clique com o botão direito no dispositivo selecionado (ou até 20 dispositivos multiselecionados) e, a seguir clique em **Analisar LANDesk Antivirus agora**.
2. Selecione configurações de antivírus.
3. Especifique se quer atualizar arquivos de definição de vírus antes e analisar. (Nota: Esta opção atualiza automaticamente os arquivos padrão de vírus antes que a análise seja iniciada, inclusive arquivos de definição de vírus que residem na pasta piloto.)
4. Clique em **OK**.

Ajuda de configurações antivírus

Sobre a caixa de diálogo Configurações do LANDesk Antivirus

Use esta caixa de diálogo para criar e editar uma configurações de antivírus. Configurações de antivírus determinam se o ícone LANDesk Antivirus aparece na bandeja do sistema do dispositivo, disponibilidade de opções interativas para usuários finais, verificação de email e ativação de proteção em tempo real, tipos de arquivos para verificar, arquivos e pastas para excluir, quarentena de arquivo infectado e Backup, verificação agendada de antivírus, e definições de atualizações de vírus agendados.

Se desejar modificar as definições padrão de antivírus de um dispositivo sem a redistribuição de uma tarefa de análise antivírus, faça a sua mudança em qualquer uma das definições nas várias páginas da caixa de diálogo Definições de antivírus, designe a novas definições para uma tarefa de definições de mudança e distribua essa tarefa aos dispositivos alvo.

Quando configuradas, você poderá aplicar as definições de antivírus às tarefas de análise e de definições de mudança.

Esta caixa de diálogo contém as seguintes páginas:

- "Sobre o Antivirus: Página de configurações gerais" na página 741
- "Sobre o Antivirus: Página de proteção em tempo real" na página 742
- "Sobre o Antivirus: Página de análise de vírus" na página 744
- "Sobre o Antivirus: Página de análise agendada" na página 746
- "Sobre o Antivirus: Página de atualizações das definições de vírus" na página 747
- "Sobre o Antivirus: Página para atualizações das definições herdadas de vírus" na página 749
- "Sobre o Antivirus: Página Quarentena/Backup" na página 749

Sobre o Antivirus: Página de configurações gerais

Use esta página para configurar as definições básicas do analisador de antivírus nos dispositivos alvo.

Essa página contém as seguintes opções:

- **Nome:** identifica as definições de antivírus com um nome exclusivo. Este nome é exibido na lista suspensa em uma caixa de diálogo de tarefa de análise antivírus.
- **Mostrar ícone do LANDesk Antivirus na janela do sistema:** Coloca o ícone do LANDesk Antivirus na bandeja do sistema do dispositivo. A aparência do ícone depende do status da proteção de antivírus, indicando se a proteção em tempo real está ativada. Se o ícone de flecha for amarelo, a proteção em tempo real está ativada, o que significa que o dispositivo está sendo monitorado continuamente contra vírus. Se o ícone estiver acinzentado, a proteção em tempo real não está habilitado.

  NOTA: Os usuários finais podem clicar duas vezes no ícone para abrir o cliente LANDesk Antivirus e executar tarefas. Eles também podem clicar com o botão direito no ícone para acessar o menu de atalho e selecionar a execução de uma análise e atualizar os arquivos de antivírus.

- **Ativar análise de email:** Ativa a análise de email nos dispositivos alvo em tempo real. A análise de email contínua em tempo real monitora a entrada e saída de mensagens (dentre os aplicativos suportados está o Microsoft Outlook), verificando a existência de vírus no corpo da mensagem e em quaisquer mensagens e arquivos anexados. Os vírus detectados são removidos.

- **Habilitar análise com o clique do botão direito:** Fornece uma opção no cliente LANDesk Antivirus permitindo os usuários finais selecionar um arquivo, grupo de arquivos, pasta ou grupo de pastas e clicar com o botão direito na seleção para fazer uma análise antivírus.
- **Analisar software de risco além de vírus (banco de dados estendido):** Fornece uma opção no cliente LANDesk Antivirus permitindo aos usuários finais analisar software de risco (por exemplo, FTP, IRC, utilitários de controle remoto, etc.) usando um banco de dados estendido que é carregado no dispositivo gerenciado.
- **Permitir ao usuário adicionar arquivos e pastas à lista de Itens confiáveis:** Fornece uma opção no cliente LANDesk Antivirus permitindo aos usuários identificar arquivos e pastas que não devem receber a análise de vírus. Os arquivos e as pastas nessa lista são ignorados pela análise antivírus. Os usuários devem estar cientes de que devem mover somente arquivos seguros para essa lista de itens confiáveis.
- **Uso da CPU durante a análise:** Permite controlar o uso da CPU em computadores alvo durante a análise antivírus pelo LANDesk Antivirus.
- **Proprietário:** Permite especificar um proprietário para as configurações do antivírus a fim de impedir modificações não autorizadas. Somente o proprietário e os usuários com o direito de Administrador LanDesk podem acessar e modificar as configurações. Outros usuários só poderão ver as configurações. A opção de usuário público permite o acesso universal às configurações.
- **Definir como padrão:** Estabelece essas definições de antivírus (inclusive as definições de opção em todas as guias da caixa de diálogo Definições de antivírus) como padrão nos dispositivos alvo. A não ser que uma tarefa de análise antivírus tenha definições específicas de antivírus a ela associada, as definições padrão são usadas durante a análise e tarefas de atualização de arquivo de definição.
- **Restaurar padrões:** Restaura as definições padrão pré-definidas para todas as opções de antivírus nas guias da caixa de diálogo.

Sobre o Antivirus: Página de proteção em tempo real

Use essa página para ativar e configurar a proteção de arquivos em tempo real, quais arquivos proteger e o que excluir, e a notificação do usuário final.

A proteção em tempo real é uma análise contínua (segundo plano) dos arquivos especificados, pastas e tipos de arquivos por extensão. Quando a proteção em tempo real estiver em execução, os arquivos serão analisados para a detecção de vírus toda vez que forem abertos, fechados, acessados, copiados ou salvos.

Quando a proteção em tempo real é ativada, o ícone de bandeja do sistema do LANDesk Antivirus é amarelo. O ícone permanece esmaecido quando a proteção em tempo real está desligada.

Essa página contém as seguintes opções:

- **Habilitar a proteção de arquivo em tempo real:** Ativa a proteção de arquivo em tempo real nos dispositivos gerenciados. A proteção de arquivo em tempo real é executada em segundo plano e procura vírus conhecidos de acordo com os arquivos carregados de definição de vírus
- **Mostrar mensagens em tempo real no cliente:** Mostra mensagens nos dispositivos alvo para notificar os usuários de determinadas atividades do LANDesk Antivirus. Usuários finais são notificados quando um arquivo infectado é detectado, colocado em quarentena, excluído, pulado ou limpo. Caixas de diálogos de mensagem mostram o caminho, nome de arquivo, nome do vírus e uma observação informando o usuário final para contatar o administrador da rede.

- **Permitir ao usuário desativar a análise em tempo real até:** Fornece uma opção no cliente LANDesk Antivirus permitindo ao usuário final desligar a proteção de arquivo em tempo real por um período especificado. Mantenha o período mínimo para que os usuários não desabilitem a proteção em tempo real por um período longo.
- **Excluir caminhos de rede:** Limita a análise de arquivo em tempo real para unidades locais e não inclui unidade de rede mapeada.
- **Analisar todos os tipos de arquivos:** Especifica que os arquivos de todos os tipos no dispositivo alvo são analisados por uma análise antivírus. Como isso pode levar bastante tempo, é aconselhado analisar todos os tipos de arquivos em uma análise em demanda em vez de proteção em tempo real.
- **Só analisar arquivos infectáveis:** Especifica que somente os arquivos infectáveis são analisados. Arquivos infectáveis são de tipo vulneráveis a infecções de vírus. Analisar somente os arquivos infectáveis é mais eficiente do que analisar todos os arquivos porque alguns vírus afetam somente certos tipos de arquivos. No entanto, certifique-se de verificar regularmente todos os arquivos com um análise por demanda para garantir que os dispositivos permaneçam limpos.

  NOTA: Os tipos de arquivos infectáveis são determinados por seus identificadores de formato no cabeçalho de cada arquivo, e não pela extensão do arquivo, para garantir que os arquivos renomeados sejam analisados. Os arquivos infectáveis incluem: arquivos de documentos como Word e Excel; arquivos modelo associados a arquivos de documento e arquivos de programa como dynamic link libraries (.DLLs), arquivos de comunicação (.COM), arquivos executáveis (.EXEs) e outros arquivos de programa. Veja abaixo uma lista compoleta dos tipos de arquivos infectáveis.

- **Usar heurística para analisar arquivos suspeitos:** Usa a capacidade de análise heurística do analisador ao analisar dispositivos alvo. A análise heurística tenta detectar arquivos dos quais se suspeita terem sido infectados por um vírus ao procurar por um comportamento suspeito, como por exemplo, um programa que: seja auto-modificável tentando encontrar outros executáveis ou que é modificado após o encerramento. (NOTA: O uso de análise heurística pode afetar negativamente o desempenho em dispositivos gerenciados.)
- **Excluir os seguintes arquivos e pastas:**
  - **Adicionar:** Abre a caixa de diálogo **Adicionar caminho excluído** onde você poderá criar novas exclusões para especificar os arquivos, as pastas ou os tipos de arquivos (por extensão) que desejar excluir de uma análise antivírus associada a essas definições.
  - **Editar:** Abre a exclusão selecionada para você modificar um caminho de arquivo, nome de arquivo, extensão de arquivo e variáveis.
  - **Excluir:** Remove a exclusão selecionada das definições de antivírus.

Sobre a caixa de diálogo Adicionar caminho excluído

Use este diálogo (acessado da caixa de diálogo de proteção em tempo real) para adicionar exclusões que especificam objetos não analisados por uma análise antivírus ou proteção em tempo real. As tarefas de análise antivírus (e tarefas de definições de mudança) associadas a essas configurações de antivírus usarão essas exclusões.

Você pode excluir arquivos específicos, pastas inteiras e tipos de arquivos por suas extensões.

Esta caixa de diálogo contém as seguintes opções:

- **Tipo:** Indica o tipo de objeto que você deseja excluir da análise antivírus. Selecione um tipo e digite os atributos corretos no campo Objeto.

- **Objeto:** Digite o nome e caminho completos (ou busque-os e selecione-os) do arquivo ou pasta que deseja excluir. Se você selecionou o tipo de extensão de arquivo, digite os caracteres da extensão no campo Objeto.
- **Inserir variável:** Permite usar as variáveis de ambiente do sistema para identificar o caminho a uma pasta ou objeto que deseja excluir da análise antivírus ou escopo de proteção.

Sobre o Antivirus: Página de análise de vírus

Use essa página para especificar quais arquivos analisar em busca detecção de vírus, o que excluir da análise e se heurística deve ser usada na análise de arquivos suspeitos.

Essa página contém as seguintes opções:

- **Analisar todos os tipos de arquivos:** Especifica que os arquivos de todos os tipos no dispositivo alvo são analisados por uma análise antivírus. Como isso pode levar bastante tempo, é aconselhado analisar todos os tipos de arquivos em uma análise em demanda em vez de proteção em tempo real.
- **Só analisar arquivos infectáveis:** Especifica que somente os arquivos infectáveis são analisados. Arquivos infectáveis são de tipo vulneráveis a infecções de vírus. Analisar somente os arquivos infectáveis é mais eficiente do que analisar todos os arquivos porque alguns vírus afetam somente certos tipos de arquivos. No entanto, certifique-se de verificar regularmente todos os arquivos com um análise por demanda para garantir que os dispositivos permaneçam limpos. Veja abaixo uma lista compoleta dos tipos de arquivos infectáveis.
- **Usar heurística para analisar arquivos suspeitos:** Usa a capacidade de análise heurística do analisador ao analisar dispositivos alvo. A análise heurística tenta detectar arquivos dos quais se suspeita terem sido infectados por um vírus ao procurar por um comportamento suspeito, como por exemplo: um programa auto-modificável tentando encontrar outros executáveis ou que é modificado após o encerramento. O uso de análise heurística pode afetar negativamente o desempenho em dispositivos gerenciados.
- **Excluir os seguintes arquivos e pastas**
  - **Adicionar:** Abre a caixa de diálogo **Adicionar caminho excluído** onde você poderá criar novas exclusões para especificar os arquivos, as pastas ou os tipos de arquivos (por extensão) que desejar excluir de uma análise antivírus associada a essas definições.
  - **Editar:** Abre a exclusão selecionada para você modificar um caminho de arquivo, nome de arquivo, extensão de arquivo e variáveis.
  - **Excluir:** Remove a exclusão selecionada das definições de antivírus.
- **Limpar registro:** Especifica se o registro está incluso na análise de antivírus.

IMPORTANTE: Análise de ponto de restauração do sistema
O LANDesk Antivirus analisará os arquivos em qualquer pasta de ponto de restauração de sistema que possam existir no dispositivo gerenciado.

Tipos de arquivos infectáveis

Os tipos de arquivos infectáveis são determinados por seus identificadores de formato no cabeçalho de cada arquivo, e não pela extensão do arquivo, para garantir que os arquivos renomeados sejam analisados.

Os arquivos infectáveis incluem: arquivos de documentos como Word e Excel; arquivos modelo associados a arquivos de documento e arquivos de programa como dynamic link libraries (.DLLs), arquivos de comunicação (.COM), arquivos executáveis (.EXEs) e outros arquivos de programa. Veja abaixo uma lista dos tipos de arquivos infectáveis pela extensão padrão ou original do formato do arquivo.

- ACM
- ACV
- ADT
- AX
- BAT
- BIN
- BTM
- CLA
- COM
- CPL
- CSC
- CSH
- DLL
- DOC
- DOT
- DRV
- EXE
- HLP
- HTA
- HTM
- HTML
- HTT
- INF
- INI
- JS
- JSE
- JTD
- MDB
- MSO
- OBD
- OBT
- OCX
- PIF
- PL
- PM
- POT
- PPS
- PPT
- RTF
- SCR
- SH

- SHB
- SHS
- SMM
- SYS
- VBE
- VBS
- VSD
- VSS
- VST
- VXD
- WSF
- WSH

Sobre o Antivirus: Página de análise agendada

Use esta página para ativar e configurar uma análise recorrente agendada de antivírus nos dispositivos alvo.

NOTA: Tipos de análise do LANDesk Antivirus
Você pode analisar os dispositivos gerenciados para encontrar vírus com análises agendadas, análises em demanda, e proteção em tempo real de arquivos e email. Os usuários finais também podem fazer análises em demanda em seus computadores.

Essa página contém as seguintes opções:

- **Análise do LANDesk Antivirus nos dispositivos para detectar vírus em horas agendadas:** Ativa uma análise antivírus recorrente agendada que é executada nos dispositivos alvo de acordo com a hora de início, freqüência, restrição de tempo e requisitos de largura de banda por você especificados.
- **Mudar configurações:** Abre a caixa de diálogo Agendar onde poderá especificar as opções de agendamento. Consulte "Sobre a caixa de diálogo Agendar análises periódicas de antivírus" na página 746.
- **Permitir ao usuário agendar análises:** Permite que o usuário final crie uma análise antivírus agendada local em seu próprio computador.

Sobre a caixa de diálogo Agendar análises periódicas de antivírus

Se desejar que essas definições de antivírus inclua uma análise recorrente, use essa caixa de diálogo para especificar a hora de início, frequência, restrição de tempo e definições necessárias da largura de banda. As tarefas de análise antivírus (e tarefas de definições de mudança) associadas a essas configurações usarão as regras aqui definidas.

Todos os critérios na configuração desta caixa de diálogo devem ser satisfeitos antes da tarefa executar. Por exemplo, se você configurar um horário que se repetir todos os dias entre as 8 e 9 com o **Estado do computador** em **Desktop deve estar bloqueado**, a tarefa somente executará se for entre 8 e 9 E o computador estiver bloqueado.

Esta caixa de diálogo contém as seguintes opções:

- **Iniciar:** Clique esta opção para exibir um calendário onde pode selecionar o dia que você quer que a tarefa inicie. Uma vez escolhido o dia, você pode também digitar uma hora do dia. Estas opções são

definidas à data e hora atual.

- **Repetir depois de:** Agenda a análise a ser repetida periodicamente. Selecione o número de minutos, horas e dias para controlar a freqüência de repetição da tarefa.
- **Intervalo de tempo:** Se desejar que a tarefa execute em horas específicas, selecione as horas de início e final. As horas estão no formato de 24 horas (militar).
- **Semanalmente entre:** Se desejar que a tarefa execute em dias específicos da semana, selecione os dias de início e final.
- **Mensalmente entre:** Se desejar que a tarefa execute em datas específicas do mês, selecione as datas de início e final.
- **Largura de banda mínima:** Ao configurar comandos do planejador local, você pode especificar os critérios mínimos de largura de banda necessários para a execução da tarefa. O teste de largura de banda consiste no tráfego da rede para o dispositivo que você especificar. Quando for o momento de execução da tarefa, cada dispositivo que estiver executando a tarefa do planejador local enviará uma pequena quantidade de tráfego de rede de ICMP para o dispositivo que você especificar e avaliará o desempenho. Se o dispositivo alvo de teste não estiver disponível, a tarefa não será executada. Você pode selecionar as seguintes opções mínimas de largura de banda:
  - **RAS:** A tarefa é executada se a conexão de rede do dispositivo ao dispositivo alvo possuir pelo menos RAS ou velocidade de dial-up, conforme detectado pela API de rede. A seleção dessa opção, em geral, significa que a tarefa sempre será executada se o dispositivo tiver algum tipo de conexão de rede.
  - **WAN:** A tarefa será executada se a conexão do dispositivo ao dispositivo alvo possuir pelo menos velocidade de WAN. Velocidade WAN é definida como uma conexão não RAS que é mais lenta que o limite da LAN.
  - **LAN:** A tarefa será executada se a conexão do dispositivo ao dispositivo alvo exceder os parâmetros de velocidade de LAN. Por padrão, a velocidade é definida como qualquer valor acima de 262.144 bps. Você pode definir o limite da LAN na configuração do agente (página **Ferramentas > Configuração > Configuração do agente, Detecção de largura de banda**). As mudanças não terão efeito até você distribuir a configuração atualizada aos dispositivos.
  - **Para o nome do computador:** Identifica o computador usado para testar a largura de banda do dispositivo. A transmissão de teste é entre o dispositivo alvo e esse computador.
- **Estado da máquina:** Se você quiser que os critérios de execução da taerfa inclua um estado de computador, selecione um da lista suspensa.
- **Atraso aleatório adicional uma vez que os outros filtros forem aprovados:** Se desejar um atraso aleatório adicional, use esta opção. Se selecionar um atraso aleatório que ultrapassa os limites de tempo configurados para a tarefa, a tarefa pode não executar se o valor aleatório colocar a tarefa fora dos limites de tempo configurados.
  - **Atrasar até:** Selecione o atraso aleatório adicional que desejar.
  - **E pelo menos:** Se desejar que a tarefa aguarde pelo menos um número específico de minutos antes de executar, selecione esta opção. Por exemplo, se estiver agendando uma varredura de inventário, você pode digitar cinco aqui para o computador ter tempo de concluir a inicialização antes da varredura iniciar, melhorando assim a resposta do computador para o usuário.

Sobre o Antivirus: Página de atualizações das definições de vírus

Use essa página para configurar o agendamento de atualizações de arquivos (padrão) de definição de vírus, opções de descarregamento de usuário e acessar opções para dispositivos alvo com definições de antivírus.

Essa página contém as seguintes opções:

- **Descarrega a versão piloto dos arquivos de definição de vírus:** Descarrega arquivos de definição de vírus da pasta de teste piloto em vez do repositório padrão (\LDLogon\Antivirus\Bases) no servidor núcleo. As definições na pasta piloto podem ser descarregadas por usuários restritos com o propósito de testar as definições de vírus antes da distribuição dos mesmos à toda a rede. Quando você criar uma tarefa de análise antivírus, poderá escolher o descarregamento das últimas atualizações de definições de vírus, inclusive os residentes na pasta de teste piloto, e depois associar as definições de antivírus com essa opção habilitada para assegurar que as máquinas teste recebam os últimos arquivos conhecidos de definição de vírus. Se essa opção for selecionada, os arquivos de definição de vírus na pasta padrão (\LDLogon\Antivirus\Bases) não são descarregados.
- **Usuários podem carregar as atualizações de definição de vírus:** Dá aos usuários finais nos dispositivos alvo a opção de fazer o descarregamento dos arquivos de definição de vírus por eles mesmos. Esta opção aparece no cliente LANDesk Antivirus e pode ser acessada a partir dessa caixa de diálogo assim como clicando-se com o botão direito no ícone da bandeja do sistema LANDesk Antivirus.

  NOTA: Quando um usuário final descarrega uma atualização de arquivos de definição de vírus, o dispositivo tenta conectar a servidores na seguinte ordem: 1) servidor preferencial (se um estiver configurado); 2) servidor núcleo; 3) LANDesk Security Suite servidor de conteúdo (Internet).
- **Download das atualizações das definições de vírus a partir de:** Especifica o site de origem do qual os arquivos de definição vírus são descarregados. Dependendo da opção que você selecionar na lista suspensa aqui, uma ou ambas as opções de site de origem de download (servidor núcleo e servidor de conteúdo de segurança de Internet) descritas abaixo serão habilitadas e podem ser configuradas. (**NOTA:** As opções de download da Internet são configuradas na página **Atualizações das definições herdadas de vírus**.)
- **Opções de download do núcleo:** Permite configurar as definições do servidor núcleo se você tiver selecionado uma das opções de site de origem acima que inclui o núcleo.
  - **Desativar download de parceiro:** Impede downloads de arquivos de definição de vírus através de download de parceiro (o cache local ou um parceiro no mesmo domain de multidifusão).
  - **Desativar servidor preferencial:** Impede os downloads de arquivos de definição de vírus através de um servidor preferencial. Para obter mais informações sobre servidores preferenciais, consulte "Distribuição de softwares/Distribuição de pacotes/Métodos de entrega" na página 258
- **Agendar atualizações de definição de vírus:** Ativa uma atualização agendada recorrente de arquivo de definição de vírus que é executada nos dispositivos alvo de acordo com a hora de início, freqüência, restrição de tempo e requisitos de largura de banda por você especificados.
- **Alterar agendamento:** Abre a caixa de diálogo Agendar onde você pode especificar as opções de agendamento.

Sobre a caixa de diálogo Agendar atualizações periódicas de antivírus

Se desejar que essas definições de antivírus inclua uma atualização recorrente de definição de vírus, use essa caixa de diálogo para especificar a hora de início, freqüência, restrição de tempo e definições necessárias da largura de banda. As tarefas de análise antivírus (e tarefas de definições de mudança) associadas a essas configurações usarão as regras aqui definidas.

Para obter mais informações sobre as opções, consulte "Sobre a caixa de diálogo Agendar análises periódicas de antivírus" na página 746 acima pois esta é uma caixa de diálogo comum.

Sobre o Antivirus: Página para atualizações das definições herdadas de vírus

Use esta página para ajustar as configurações de atualização das definições herdadas, assim como as configurações do conteúdo do servidor LANDesk Security Suite se você tiver selecionado uma das opções de site de origem acima que inclui a Internet.

Essa página contém as seguintes opções:

- **Descarregar as atualizações como um arquivo único se a mudança de contagem de arquivos for maior que :** Especifica o número máximo de novos arquivos de definição de vírus individuais atualizados que são baixados separadamente, antes de serem compactados e baixados como um arquivo único.
- **Opções de download da Internet:** Permite configurar as definições de segurança do servidor de conteúdo se você tiver selecionado uma das opções de site de origem acima que inclua a Internet.
    - **Site de origem:** Especifica o servidor de conteúdo de segurança que é acessado para download das últimas definições para o seu banco de dados. Selecione o servidor mais próximo do local onde você se encontra.
    - **Ir para um site de origem alternativo se houver falha:** Tenta fazer download automaticamente das atualizações de outro servidor de conteúdo de segurança onde residemas assinaturas de antivírus se o site de origem especificado não conseguir transmitir os arquivos.

IMPORTANTE: As configurações herdadas são aplicáveis somente para clientes LANDesk Antivirus mais antigos
As configurações de atualização de das definições de antivírus herdadas especificadas nesta página são válidas somente para versões mais antigas do cliente LANDesk Antivirus que foram distribuídas para seus dispositivos gerenciados. Normalmente, as versões mais antigas do cliente são instaladas por um servidor núcleo LANDesk versão 8.8 SP3 ou mais antigo.

Sobre o Antivirus: Página Quarentena/Backup

Use essa página para configurar o tamanho da pasta quarentena/backup e as opções de restauração de objeto que desejar tornar disponível aos usuários finais.

Essa página contém as seguintes opções:

- **Limitar o tamanho da pasta quarentena/backup:** Permite a especificação do tamanho máximo da pasta compartilhada quarentena\backup nos dispositivos alvo. Essa pasta é uma área de armazenamento segura e isolada nos dispositivos com o LANDesk Antivirus. O tamanho de armazenamento da quarentena é de 50 MB e objetos em quarentena são armazenados por 90 dias, por padrão. Os objetos na pasta de quarentena\backup podem ser reanalisados, excluídos ou restaurados.

  NOTA: Arquivos em quarentena são reanalisados automaticamente com as últimas definições de vírus sempre que uma análise por demanda é executada ou quando os arquivos padrão de antivírus são atualizados no dispositivo, para descobrir se objetos infectados podem ser limpos. Se um arquivo em quarentena puder ser limpo, ele é restaurado automaticamente e o usuário é notificado.

  NOTA: Quando uma infecção de vírus é descoberta, primeiro é feito o backup do arquivo infectado (com uma extensão *.bak na pasta \LDClient\Antivirus\) e é então limpo. Se não puder ser desinfectado, o arquivo original será movido para a pasta de quarentena (com uma extensão *.qar na pasta \LDClient\Antivirus). Em seguida, a string de vírus é removida e o arquivo é criptografado para

não ser acessado ou executado.

- **Tamanho máximo:** Especifica o tamanho máximo da pasta compartilhada quarentena/backup nos dispositivos com o agente do LANDesk Antivirus.
- **Restaurar objetos:** Especifica os direitos de usuário final para restaurar objetos que foram quarentenados.
    - **Permitir ao usuário restaurar objetos suspeitos:** Fornece aos usuários finais a opção de restaurar objetos suspeitos detectados através de uma análise antivírus ou por proteção em tempo real. Objetos suspeitos são aqueles com código modificado ou remanescente a um vírus conhecido. Os objetos suspeitos são automaticamente colocados em quarentena. Se essa opção for selecionada, os usuários finais podem mover o arquivo original da pasta de quarentena a uma pasta de destino especificada ou ao seu local original, onde foi armazenado antes da quarentena, desinfecção ou exclusão. Observe que se a proteção em tempo real estiver em execução, o arquivo restaurado será analisado - e se ainda estiver infectado, é colocado de volta em quarentena.
    - **Permitir ao usuário restaurar objetos infectados e software de risco:** Fornece aos usuários finais a opção de restaurar objetos infectados, detectados através de uma análise antivírus ou por proteção em tempo real. Objetos infectados são aqueles com código danoso, detectado por um arquivo de definição de vírus conhecido (padrão ou assinatura). Objetos infectados podem danificar ainda mais os dispositivos gerenciados. O software arriscado é essencialmente um software cliente com a possibilidade de oferecer riscos ao usuário final. Por exemplo: FTP, IRC, MIrc, RAdmin ou softwares de utilitário de controle remoto. (No caso de um resultado positivo falso de análise, o usuário final pode ter a confiança suficiente para restaurar o arquivo. Essa opção permite aos usuários restaurarem arquivos nos compartilhamentos de rede. Se eles restaurarem um arquivo infectado para o local original, a próxima análise antivírus detectará o mesmo vírus, mesmo se se tratar de um positivo falso e colocará os arquivos de volta na quarentena.)
    - **Usuário deve digitar senha para restaurar objetos:** Requer que os usuários digitem a senha especificada para poderem restaurar objetos suspeitos ou infectados, ou ainda software de risco. O usuário recebe um aviso para digitar a senha quando tentar restaurar o objeto da pasta de quarentena/backup. Se ativar essa opção para proteger com senha os objetos em quarentena, deverá compartilhar essa senha com os usuários para poderem restaurar esses objetos.
    - **Senha:** Digite a senha necessária para os usuários restaurarem os objetos em quarentena.
- **Excluir arquivos:** Especifica se os arquivos são excluídos automaticamente.
    - **Excluir automaticamente arquivos em quarentena:** Indica que todos os arquivos em quarentena mais velhos que o período especificado serão automaticamente excluídos.
    - **Excluir automaticamente arquivos em backup:** Indica que todos os arquivos em backup mais velhos que o período especificado serão automaticamente excluídos.

Ajuda do LANDesk Antivirus Ultimate

LANDeskAs características do Antivirus Ultimate são acessadas pela janela ferramenta Configurações de agente. (**Ferramentas > Segurança e conformidade > Configurações de agente**).

O Antivirus permite o download e o gerenciamento do conteúdo de antivírus (arquivos de definição de vírus), a configuração de análises de antivírus, a personalização das definições de tela/interação do analisador de antivírus que determinam a maneira do analisador ser exibido e funcionar nos dispositivos alvo e quais opções interativas são disponíveis aos usuários finais. Você também pode ver informações para os dispositivos analisados, habilitar alertas e gerar relatórios de antivírus.

A principal seção do "LANDesk Antivirus" na página 712 introduz essa ferramenta de gerenciamento complementar de segurança, a qual é um componente de ambos LANDesk Management Suite e LANDesk Security Suite. Esta seção contém uma visão geral, informações de assinatura do conteúdo de antivírus e instruções detalhadas sobre como usar os recursos do LANDesk Antivirus.

Essa seção contém os seguintes tópicos de ajuda que descreve as mensagens do Antivirus. Pela interface do console, esses tópicos de ajuda são acessados clicando no botão **Ajuda** em suas respectivas caixas de diálogo.

Sobre o LANDesk Antivirus Ultimate: Página geral

Usar essa página para configurar o verificador de configurações LANDesk Antivirus em dispositivos alvo.

Essa página contém as seguintes opções:

- **Nome:** identifica as definições de antivírus com um nome exclusivo. Este nome é exibido na lista suspensa em uma caixa de diálogo de tarefa de análise antivírus.
- **Proteção:**
  - **Antivírus de arquivos:** Habilita a verificação em tempo real de arquivos nos dispositivos alvo.
  - **Antivírus para e-mails:** Ativa a análise de email nos dispositivos alvo em tempo real. A análise de email contínua em tempo real monitora a entrada e saída de mensagens (dentre os aplicativos suportados está o Microsoft Outlook), verificando a existência de vírus no corpo da mensagem e em quaisquer mensagens e arquivos anexados. Os vírus detectados são removidos.
  - **Antivírus na Web:** Habilita a verificação em tempo real do tráfego de rede, sites URLs, e links em dispositivos alvo.
  - **Antivírus em bate-papos (IM):** Habilita a verificação em tempo real de mensagens instantâneas nos dispositivos alvo.
  - **Bloqueador de ataques à rede:** Habilita o Bloqueador de ataques à rede que detecta e adiciona computadores de ataque à lista de dispositivos bloqueados por um período específico de tempo.
  - **System Watcher:** Habilita a ferramenta System Watcher a atividade de aplicativos em dispositivos alvo.
- **Permissões:**
  - **Permitir que o usuário desative componentes de proteção até:** Especifica o período de tempo durante o qual o usuário pode desligar os componentes de proteção listados acima.
  - **Permitir que o usuário atualize definições:** Permite que o usuário edite arquivos de definição do antivírus.
  - **Permitir que o usuário restaure objetos:** Deixa o usuário restaurar objetos a serem analisados.
  - **Permite que o usuário mude configurações:** Permite que o usuário agende verificações, exclua objetos de verificações, e adicione Urls de Rede.

- **Interface do usuário:**
  - **Mostrar ícone do LANDesk Antivirus na janela do sistema:** Coloca o ícone do LANDesk Antivirus na bandeja do sistema do dispositivo. A aparência do ícone depende do status da proteção de antivírus, indicando se a proteção em tempo real está ativada. Se o ícone de flecha for amarelo, a proteção em tempo real está ativada, o que significa que o dispositivo está sendo monitorado continuamente contra vírus. Se o ícone estiver acinzentado, a proteção em tempo real não está habilitado.
  - **Habilitar análise com o clique do botão direito:**
- **Definir como padrão:** Estabelece essas definições de antivírus (inclusive as definições de opção em todas as guias da caixa de diálogo Definições de antivírus) como padrão nos dispositivos alvo. A não ser que uma tarefa de análise antivírus tenha definições específicas de antivírus a ela associada, as definições padrão são usadas durante a análise e tarefas de atualização de arquivo de definição.

Sobre o LANDesk Antivirus Ultimate: Página de proteção

Use esta página para configurar as configurações de proteção.

Essa página contém as seguintes opções:

- **Iniciar LANDesk Antivirus ao iniciar o computador:**
- **Ativar a Tecnologia de desinfecção avançada:**
- **Ameaças:**
  - **Malware:**
  - **Adware, discadores automáticos, outros programas:**
  - **Arquivos compactados:**
- **Exclusões:**
  - **Tempo real:**
  - **Análise de vírus:**
- **Adicionar:**
- **Editar:**
- **Excluir:**

Sobre a caixa de diálogo Adicionar caminho excluído

Use este diálogo (acessado da caixa de diálogo de proteção em tempo real) para adicionar exclusões que especificam objetos não analisados por uma análise antivírus ou proteção em tempo real. As tarefas de análise antivírus (e tarefas de definições de mudança) associadas a essas configurações de antivírus usarão essas exclusões.

Você pode excluir arquivos específicos, pastas inteiras e tipos de arquivos por suas extensões.

Esta caixa de diálogo contém as seguintes opções:

- **Tipo:** Indica o tipo de objeto que você deseja excluir da análise antivírus. Selecione um tipo e digite os atributos corretos no campo Objeto.
- **Objeto:** Digite o nome e caminho completos (ou busque-os e selecione-os) do arquivo ou pasta que deseja excluir. Se você selecionou o tipo de extensão de arquivo, digite os caracteres da extensão no campo Objeto.

- **Inserir variável:** Permite usar as variáveis de ambiente do sistema para identificar o caminho a uma pasta ou objeto que deseja excluir da análise antivírus ou escopo de proteção.

Sobre o LANDesk Antivirus Ultimate: Página do Antivírus de arquivos

Usar essa página para configurar...

Essa página contém as seguintes opções:

- **Habilitar Antivírus de arquivos:**
- **Nível de segurança:**
  - **Geral:** Tipos de arquivos, escopo de proteção, ...
  - **Desempenho:** Análises heurísticas, verificar somente arquivos novos e modificados, verificar arquivos, verificar instalações, verificar objetos OLE incorporados, extras...
  - **Extras:** Modo de verificação, tecnologias de verificação....
- **Ação:**
  - **Selecionar ação automaticamente:**
  - **Selecionar ação:**
  - **Desinfectar:**
  - **Excluir se a desinfecção falhar:**

Sobre o LANDesk Antivirus Ultimate: Página do Antivírus de correspondências

Usar essa página para configurar...

Essa página contém as seguintes opções:

- **Habilitar Antivírus de correspondência:**
- **Nível de segurança:**
  - **Geral:** Escopo de proteção, POP3 / SMTP / NNTP / IMAP, Extra: Plug-in do Microsoft Office Outlook, adicional: Plug-in do The Bat, verificação de arquivos anexados...
    - **Escopo de proteção:** Mensagens de entrada e saída, somente mensagens de entrada...
    - **Tráfego POP3 / SMTP / NNTP / IMAP:**
    - **Extras: Plug-in do Microsoft Office Outlook:**
    - **Extras: Plug-in do The Bat!:**
    - **Verificar arquivos anexados:** Não verificar arquivos maiores que (MB), Não verificar arquivos por mais de (segundo) ...
  - **Extras:** Análises heurísticas (verificação leve, verificação média, verificação profunda...)
- **Ação:**
  - **Selecionar ação automaticamente:**
  - **Selecionar ação:** Desinfectar, excluir se a desinfecção falhar

Sobre o LANDesk Antivirus Ultimate: Página do antivírus da web

Usar essa página para configurar...

Essa página contém as seguintes opções:

- **Habilitar antivírus da web:**
- **Nível de segurança:**
- **Verificar métodos e otimização:**
  - **Verifique se os links estão listados no banco de dados de URLs suspeitos:**
  - **Verificar se os links estão listados no banco de dados de URLs de phishing:**
  - **Análise heurística para detectar vírus:**
  - **Análise heurística para links de phishing:**
  - **Limitar tempo de cache do tráfego da web:**
- **URLs confiáveis:**
  - **Não verificar tráfego Web de URLs confiáveis:**
  - **Adicionar:**
  - **Editar:**
  - **Excluir:**
- **Ação:**
  - **Selecionar ação automaticamente:**
  - **Bloquear download:**
  - **Permitir download:**

Sobre o LANDesk Antivirus Ultimate: Página do Antivírus do bate-papo

Usar essa página para configurar...

Essa página contém as seguintes opções:

- **Habilitar antivírus do bate-papo:**
- **Escopo de proteção:**
  - **Mensagens de entrada e de saída:**
  - **Somente mensagens de entrada:**
- **Métodos de análise:**
  - **Verifique se os links estão listados no banco de dados de URLs suspeitos:**
  - **Verifique se os links estão listados no banco de dados de URLs de phishing:**
  - **Análise heurística:**

Sobre o LANDesk Antivirus Ultimate: Página de bloqueador de ataque de rede:

Usar essa página para configurar...

Essa página contém as seguintes opções:

- **Habilitar bloqueador de ataques à rede:**
- **Adicionar o seguinte computador à lista de computadores bloqueados para (minutos):**

Sobre o LANDesk Antivirus Ultimate: Página do System Watcher

Usar essa página para configurar...

Essa página contém as seguintes opções:

- **Habilitar System Watcher:**
- **Atividade de aplicativo de log in de aplicativos com assinatura digital:**
- **Não monitorar a atividade de aplicativos que tenham uma assinatura digital:**
- **Reverter ações de malware:**
- **Defesa proativa:**
    - **Usar padrões atualizáveis de atividades perigosas (BSS):**
    - **Ao detectar a atividade do malware:**

Sobre o LANDesk Antivirus Ultimate: Página de tarefas agendadas

Usar essa página para configurar...

Essa página contém as seguintes opções:

- **Tarefas agendadas:**
    - **Atualizar:**
    - **Análise completa:**
    - **Análise de áreas críticas:**
- **Tarefas de análise em segundo plano:**
    - **Realizar a verificação ociosa:**
- **Verificar unidades removíveis na conexão:**
    - **Ação na conexão do disco removível:**
    - **Tamanho máximum do disco removível (MB):**

Sobre o LANDesk Antivirus Ultimate: Página de Atualização

Use essa página para configurar o agendamento de atualizações de arquivos (padrão) de definição de vírus, opções de descarregamento de usuário e acessar opções para dispositivos alvo com definições de antivírus.

Essa página contém as seguintes opções:

- **Descarrega a versão piloto dos arquivos de definição de vírus:** Descarrega arquivos de definição de vírus da pasta de teste piloto em vez do repositório padrão (\LDLogon\Antivirus\Bases) no servidor núcleo. As definições na pasta piloto podem ser descarregadas por usuários restritos com o propósito de testar as definições de vírus antes da distribuição dos mesmos à toda a rede. Quando você criar uma tarefa de análise antivírus, poderá escolher o descarregamento das últimas atualizações de definições de vírus, inclusive os residentes na pasta de teste piloto, e depois associar as definições de antivírus com essa opção habilitada para assegurar que as máquinas teste recebam os últimos arquivos conhecidos de definição de vírus. Se essa opção for selecionada, os arquivos de definição de vírus na pasta padrão (\LDLogon\Antivirus\Bases) não são descarregados.
- **Usuários podem carregar as atualizações de definição de vírus:** Dá aos usuários finais nos dispositivos alvo a opção de fazer o descarregamento dos arquivos de definição de vírus por eles mesmos. Esta opção aparece no cliente LANDesk Antivirus e pode ser acessada a partir dessa caixa de diálogo assim como clicando-se com o botão direito no ícone da bandeja do sistema LANDesk Antivirus.

  NOTA: Quando um usuário final descarrega uma atualização de arquivos de definição de vírus, o dispositivo tenta conectar a servidores na seguinte ordem: 1) servidor preferencial (se um estiver configurado); 2) servidor núcleo; 3) LANDesk Security Suite servidor de conteúdo (Internet).

- **Download das atualizações das definições de vírus a partir de:** Especifica o site de origem do qual os arquivos de definição vírus são descarregados. Dependendo da opção que você selecionar na lista suspensa aqui, uma ou ambas as opções de site de origem de download (servidor núcleo e servidor de conteúdo de segurança de Internet) descritas abaixo serão habilitadas e podem ser configuradas. (**NOTA:** As opções de download da Internet são configuradas na página **Atualizações das definições herdadas de vírus**.)
- **Opções de download do núcleo:** Permite configurar as definições do servidor núcleo se você tiver selecionado uma das opções de site de origem acima que inclui o núcleo.
    - **Desativar download de parceiro:** Impede downloads de arquivos de definição de vírus através de download de parceiro (o cache local ou um parceiro no mesmo domain de multidifusão).
    - **Desativar servidor preferencial:** Impede os downloads de arquivos de definição de vírus através de um servidor preferencial. Para obter mais informações sobre servidores preferenciais, consulte "Distribuição de softwares/Distribuição de pacotes/Métodos de entrega" na página 258
- **Agendar atualizações de definição de vírus:** Ativa uma atualização agendada recorrente de arquivo de definição de vírus que é executada nos dispositivos alvo de acordo com a hora de início, freqüência, restrição de tempo e requisitos de largura de banda por você especificados.
- **Alterar agendamento:** Abre a caixa de diálogo Agendar onde você pode especificar as opções de agendamento.

Sobre o LANDesk Antivirus Ultimate: Página completa de verificação

Usar essa página para configurar...

Essa página contém as seguintes opções:

- **Nível de segurança:**
    - **Alta:**
    - **Recomendadas:**
    - **Baixa:**
- **Escopo:**
    - **Tipos de arquivo:**
    - **Otimização da verificação:**
    - **Verificação de arquivos compostos:**
    - **Extras:**
- **Extras:**
    - **Métodos de análise:**
    - **Tecnologias de verificação:** tecnologia iSwift ou iChecker...
- **Ação:**
    - **Selecionar ação automaticamente:**
    - **Executar a ação:**

Sobre o LANDesk Antivirus Ultimate: Página de verificação de áreas críticas

Usar essa página para configurar...

Essa página contém as seguintes opções:

- **Nível de segurança:**
  - **Alta:**
  - **Recomendadas:**
  - **Baixa:**
- **Escopo:**
  - **Tipos de arquivo:**
  - **Otimização da verificação:**
  - **Verificação de arquivos compostos:**
  - **Extras:**
- **Extras:**
  - **Métodos de análise:**
  - **Tecnologias de verificação:** tecnologia iSwift ou iChecker...
- **Ação:**
  - **Selecionar ação automaticamente:**
  - **Executar a ação:**

Sobre o LANDesk Antivirus Ultimate: Página de verificação personalizada

Usar essa página para configurar...

Essa página contém as seguintes opções:

- **Nível de segurança:**
  - **Alta:**
  - **Recomendadas:**
  - **Baixa:**
- **Escopo:**
  - **Tipos de arquivo:**
  - **Otimização da verificação:**
  - **Verificação de arquivos compostos:**
  - **Extras:**
- **Extras:**
  - **Métodos de análise:**
  - **Tecnologias de verificação:** tecnologia iSwift ou iChecker...
- **Ação:**
  - **Selecionar ação automaticamente:**
  - **Executar a ação:**

Sobre o LANDesk Antivirus Ultimate: Página de configurações avançada

Usar essa página para configurar...

Essa página contém as seguintes opções:

- **Ativar autodefesa:**
- **Desativar o gerenciamento externo de serviço do sistema:**

- **Conceder recursos para outros aplicativos:**

Sobre o LANDesk Antivirus Ultimate: Página de relatórios e armazenagem

Usar essa página para configurar...

Essa página contém as seguintes opções:

- **Parâmetros de relatórios**
- **Armazenar relatórios que não ultrapassem (dias):**
- **Tamanho máximo do arquivo (MB):**
- **Configurações locais de quarentena e backup:**
  - **Reanalisar arquivos em quarentena após atualização:**
  - **Armazenar objetos que não ultrapassem:**
  - **Tamanho máximo de armazenamento:**

Sobre o LANDesk Antivirus Ultimate: Página da interface

Usar essa página para configurar...

Essa página contém as seguintes opções:

- **Exibir "Protegido pelo LANDesk Antivirus" na tela de logon do Microsoft Windows:**
- **Usar animação de ícone ao executar tarefas:**

Sobre o LANDesk Antivirus Ultimate: Página de configuração de importação

Usar essa página para configurar...

Essa página contém as seguintes opções:

- **Importar arquivo de configurações de um cliente de antivírus da Kaspersky:**
  - **Configuração atual importada de:**
  - **Limpar senha após importar:**
  - **Na data:**
  - **Notas:**

Tópicos relacionados

Ajuda do Central de ações do LANDesk Antivirus / Licenciamento

Use esta caixa de diálogo para configurar os principais recursos do LANDesk Antivirus no ambiente de rede da LANDesk.

IMPORTANTE: Chave de licença válida do LANDesk Antivirus é obrigatória
Antivírus
de LANDesk exige uma chave válida de licença para ativar o produto em seu servidor núcleo e usa a ferramenta de LANDesk Antivirus para configurar e para proteger dispositivos de alvo.

Você pode especificar a validade da licença do LANDesk Antivirus e analisar os dispositivo alvo para verificar a conformidade, importar uma nova chave válida de licença, verificar o estado da definição atual de antivírus (padrão) em seu servidor núcleo e fazer o download dos arquivos de definição do antivírus mais recentes.

Sobre a caixa de diálogo de Centro de Ação de LANDesk Antivirus

Esta caixa de diálogo contém as seguintes opções:

- **Reconhecer que outros antivírus serão removidos:** Especifica que você concorda que o processo de instalação de LANDesk Antivirus retirará qualquer outro software detectado de antivírus de apontar dispositivos.
- **Chave de licença do LANDesk Antivirus é obrigatória:** Você necessita uma licença válida de LANDesk Antivirus para instalar e usar o produto pleno de LANDesk Antivirus em sua rede.
    - **Importar nova licença:** Deixa-o importar uma chave válida de licença de LANDesk Antivirus para ativar o produto em seu servidor núcleo.
- **Verificar se algum cliente está próximo do vencimento da licença:** Você pode escanear os dispositivos administrados em sua rede configurado com LANDesk Antivirus ver se sua chave de licença é perto de sua data de vencimento.
    - **Mudar:** Deixa-o especificar o número de dias permanecendo antes que sua chave de licença de LANDesk Antivirus expira.
    - **Importar nova licença:** Deixa-o importar uma chave válida de licença de LANDesk Antivirus para ativar o produto em seu servidor núcleo.
    - **Exibir clientes:** Deixa-o ver quais dispositivos gerenciados estão dentro do limiar especificado de validade da licença do LANDesk Antivirus.
- **Definições do antivírus estão desatualizadas:** Indica que as definições de antivírus (padrão ou arquivos de assinatura) em seu servidor núcleo não são até data (de acordo com seu prazo especificado).
    - **Mudar:** Deixa-o especificar o número de dias permanecendo durante que tempo a definição existente de antivírus (padrão) arquivos atualmente residindo em seu servidor núcleo são considerados estar até data.
    - **Ir para download de atualizações:** Abre o diálogo da Ferramenta de Patch e conformidade onde você pode configurar parâmetros de download e executar (agendar) tarefas de download de arquivos de definição do antivírus.
- **Exibir esta caixa de diálogo automaticamente se forem necessárias ações do antivírus:** Capacita o diálogo de Centro de Ação de LANDesk Antivirus para exibir no console da LANDesk se qualquer dos parâmetros especificados das opções listados acima, ativante um lembrete.

Sobre a caixa de diálogo Informações da licença do LANDesk Antivirus

Use este diálogo para exibir as informações atuais da licença de LANDesk Antivirus e importe uma nova chave de licença.

IMPORTANTE: Somente LANDesk Administrators
Somente os Administradores da LANDesk podem importar uma chave de licença do LANDesk Antivirus.

Esta caixa de diálogo contém as seguintes opções:

- **Importar novo arquivo de licença:**
  - **Caminho:** Navegue à chave de licença de LANDesk Antivirus que você recebeu de LANDesk.
  - **Criado em:** Mostra a data de criação para a chave de licença.
  - **Número da licença:** Mostra o número da chave da licença.
  - **Número de informação da licença:** Mostra as informações de licença.
- **Informações da licença atual:**
  - **Caminho:** Mostra o caminho de arquivo até a chave de licença do LANDesk Antivirus.
  - **Criado em:** Mostra a data de criação para a chave de licença.
  - **Número da licença:** Mostra o número da chave da licença.
  - **Número de informação da licença:** Mostra as informações de licença.
- **Informações de distribuição:**
  - **Nós ativados:** Indica o número de dispositivos administrados que foram configurado para proteção de LANDesk Antivirus e que correm com uma chave válida de licença.
  - **Contagem máxima:** Indica o número máximo de dispositivos administrados que podem ser configurado para proteção de LANDesk Antivirus de acordo com a licença você recebeu de LANDesk e ativava o produto de LANDesk Antivirus em seu servidor núcleo.
  - **Data de validade mais próxima:** Indica a data em que o próximo conjunto de chaves de licença do LANDesk Antivirus expirará.

Proteção de dados da Credant

Visão geral do LANDesk Data Protection

O LANDesk® Data Protection com a ferramenta Credant é uma solução integrada de um parceiro que permite que você colete, monitore e veja as informações sobre a integridade de seus dispositivos gerenciados no console da LANDesk.

LANDesk Data Protection usa duas ferramentas de parceiros Credant — servidores Credant Enterprise (pré-instalados e configurados) e o software Credant agent em execução nos dispositivos gerenciados pela LANDesk.

Protegidos por serviços do Data Protection

Quando o agente Credant (Data Protection) está instalado em um dispositivo gerenciado, é considerado "protegido" pelo serviço integrado do Credant Data Protection. Servidores da Credant usam criptografia inteligente baseada em diretivas para proteger os dados em dispositivos protegidos (i.e. , os dispositivos configurados com o agente do Data Protection). A LANDesk simplesmente recolhe esta informação e envia relatórios para o banco de dados do núcleo que permite os administradores da LANDesk vejam as informações do Data Protection no modo de exibição de Inventário do console e em um relatório predefinido do Data Protection.

Criptografia de dados inteligentes possui os seguintes recursos:

- Suporta algoritmos padrão da indústria (incluindo FIPS 140-2 -validado AES 128 e AES 256)
- Complementa o Microsoft Windows BitLocker
- Depósito de chave de encriptação automática de simples e imediata recuperação de dados
- Encripta o banco de dados local e o hash da senha de domínio do Security Account Manager (SAM)

O servidor núcleo da LANDesk coleta informações do banco de dados do servidor da Credant (Data Protection) conforme determinado pelo agente do Data Protection instalado em cada dispositivo gerenciado.

IMPORTANTE: Os servidores empresariais da Credant já devem estar instalados e configurados
Para usar as novas ferramentas integradas do Data Protection e recursos do console da LANDesk, um servidor ou servidores da Credant Enterprise (Data Protection) já devem estar instalados em seu ambiente de rede da LANDesk. Em outras palavras, as tarefas de instalação e configuração do servidor da Credant devem ser realizada ANTES da configuração dos servidores no servidores no console do LANDesk (i.e. , adicionar) e de criar a conexão com o banco de dados do Data Protection com o banco de dados do núcleo da LANDesk. Vá para o site da Credant: Credant Enterprise Edition Home Page.

Recursos e benefícios

Com o LANDesk Data Protection é possível:

- Configure uma conexão entre o servidor núcleo da LANDesk e os servidores de sincronização de dados da Credant que executam a sincronização de dados entre os respectivos bancos de dados respectivos e os dispositivos protegidos e configurados na rede de LANDesk.
- Veja as informações do Data Protection no modo de exibição de Inventário da LANDesk (no nó **Data Protect**) e clique com o botão direito no modo de exibição do Resumo de inventário (resultados e dados das análises imediatas em tempo real).

- Iniciar o console Web nativo da Credant.
- Você pode usar essas informações do Data Protection obtidas dos bancos de dados da Credant (Data Protection) para criar consultas padrão que procuram atributos específicos, como você faz com todos os tipos de dados do inventário. Você também pode usar este dados com as definições padrão de colunas
- Cria tarefas agendadas que coleta automaticamente informações de todos os banco de dados da Credant (Data Protection).
- Crie um relatório do Data Protection que compila e mostra todos os dados de dispositivos protegidos em um único relatório gráfico.

NOTA: O **LANDesk Data Protection suporta múltiplos servidores e banco de dados**
Administradores tem a habilidade de reunir dados de dispositivos gerenciados de múltiplos servidores do Data Protection e de banco de dados.

Descrição das principais tarefas do Data Protection

A lista abaixo descreve as principais tarefas envolvidas na configuração, implementação e uso do Data Protection. Consulte os tópicos de ajuda específicos do recurso para obter informações conceituais e práticas detalhadas.

- Configure os servidores empresariais da Credant.
- Adicionar o servidor da Credant (Proteção de Dados) a sua rede através do console da LANDesk Management Suite.
- Crie uma conexão com o banco de dados entre o servidor da Credant (Data Protection) e o servidor do núcleo da LANDesk.
- Instale o o agente Credant nos dispositivos gerenciados
- Veja informações do Data Protection no modo de exibição de Inventário.
- Veja informações do Data Protection no modo de exibição em tempo real do Resumo.
- Gerar relatórios do Data Protection.

IMPORTANTE: NÃO interrompa o servido da Credant em seus dispositivos gerenciados
O LANDesk Data Protection melhorou o analisador de inventário para detectar se o agente da Credant está instalado no dispositivo gerenciado, os números da versão e os serviços em execução. NÃO pare o serviço da Credant porque forçará sua máquina a reiniciar.

Interface do Data Protection no dispositivo do usuário final

O nome do software do cliente do Data Protection que os usuários finais verão é:

Credant Mobile Guardian Shield

Sobre o arquivo de log do Data Protection

O arquivo de log pode ajudar administradores de sistema a solucionar problemas problemas específicos.

Onde obter mais informações

Navegue pelo tópicos de ajuda do LANDesk Management Suite na Central de ajuda LANDesk ou execute execute uma busca usando uma palavra-chave ou frase para encontrar a informação que você deseja.

A Comunidade usuários LANDesk tem fóruns de usuários e os melhores métodos conhecidos para todos os produtos e tecnologia da LANDesk. Para acessar esse recurso valioso, visite:

Página inicial da Comunidade de usuários da LANDesk

Tópicos relacionados

"Pré-requisitos do Data Protection" na página 763

"Use a ferramenta Data Protection" na página 764

"Sobre o servidor do Data Protection: Página de propriedades do servidor" na página 769

"Sobre o servidor do Data Protection: Página de conexão do banco de dados" na página 770

"Exibir as informações do Data Protection no inventário" na página 765

"Gere o relatório do Data Protection" na página 767

Pré-requisitos do Data Protection

Antes de configurar (p. exe., adicionar) servidores da Credant através do console da LANDesk, certifique-se de atender todos os prerrequisitos do sistema a seguir:

IMPORTANTE: Configuração do servidor empresarial da Credant
A LANDesk supõe que você está familiarizado com os procedimentos de instalação do produto e já realizou esta tarefa preliminar. Para obter mais informações, acesse o site da Credant em: Credant Enterprise Edition Home Page.

Pré-requisitos

Assegure-se que todos os seguintes requisitos são atendidos antes de configurar os servidores da Credant para tarefas de sincronização de dados e de obtenção de dados específicos do Data Protection através do servidor núcleo da LANDesk.

- O LANDesk Management Suite, versão 9.5, deve ser instalado em seu servidor núcleo. (Esta instalação inclui o software de servidor núcleo e o banco de dados de suporte). Para instruções detalhadas, passo a passo, de como instalar e distribuir um ambiente núcleo do servidor/banco de dados do LANDesk Management Suite, vá até a Comunidade de suporte a usuários da LANDesk em: Página inicial da Comunidade de usuários da LANDesk
- O Agente LANDesk padrão (CBA, ou Common Base Agent) versão 9.5 deve ser distribuída aos dispositivos gerenciados que você quer proteger com a ferramenta Data Protection.
- Um ou mais servidores do Credant Enterprise Edition (CEE) devem ser definidos e configurados em sua rede. Para obter instruções sobre como instalar e configurar o servidores da Credant você consultar a documentação oficial da Credant(veja o link acima).

Tópicos relacionados

"Proteção de dados da Credant" na página 761

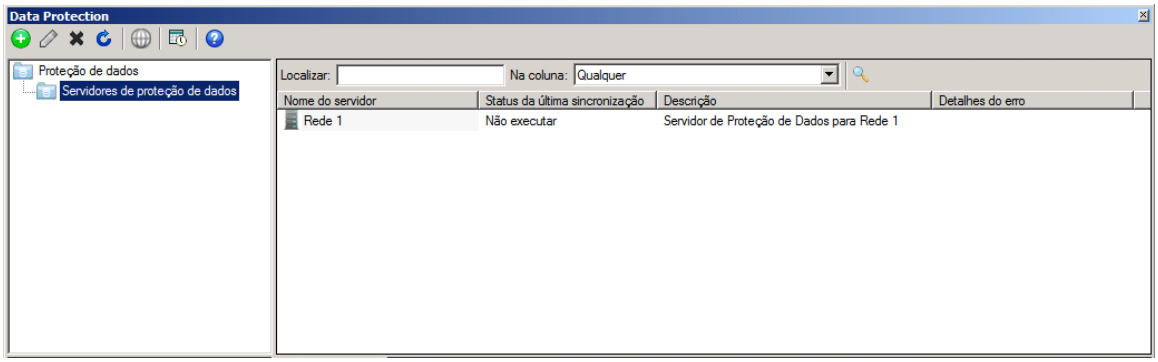
Use a ferramenta Data Protection

A ferramenta integrada do Data Protection permite que você colete, armazene, rastreie e veja informações detalhadas sobre o status da integridade dos dados nos dispositivos gerenciados na sua rede LANDesk Management Suite.

Janela da ferramenta Data Protection

Acesse a ferramenta do Data Protection no console principal da LANDesk no menu de Ferramentas (**Ferramentas > Segurança e Conformidade > Data Protection**) ou a Caixa de ferramentas.

A janela da ferramenta do Data Protection lista os servidores do Data Protection que você adicionou a sua rede. (**NOTA:** Instalando e configurando um servidor do Data Protection (Credant Enterprise) é uma tarefa separada. Você deve seguir as especificações técnicas e instruções do fornecedor para religar o servidor. Então você pode adicionar o servidor a sua rede LANDesk).



Barra de ferramentas de proteção de dados

A janela de ferramenta do Data Protection também tem os seguintes botões de barra de ferramentas:

- **Servidor de proteção de novos dados:** Permite que você adicione (configurar) um servidor existente do Data Protection a sua rede da LANDesk de modo que possa comunicar com o servidor núcleo da LANDesk e banco de dados, e envia informações sobre os dados em dispositivos gerenciados que têm o agente do Data Protection instalado.
- **Propriedades:** Exibe a página de propriedades para o servidor selecionado.
- **Excluir:** Remove o servidor selecionado selecionado do seu sistema da LANDesk.
- **Atualizar:** Recarrega todos os servidores configurados (adicionados) dos servidores do Data Protection com suas últimas mudanças.
- **Console Web (se disponível):** Inicia o aplicativo do servidor Web da Credant em um navegador (se o servidor especificado tem este software instalado como parte de sua configuração). O console Web da Credant exibe somente informações específicas da Credant, sem nenhum conteúdo integrado da LANDesk. (**NOTA:** O Silverlight deve estar instalado para visualizar o servidor Web.)
- **Agendar tarefa de sincronização:** Cria uma tarefa agendada que sincroniza os dados de TODOS os servidores do Data Protection que você adicionou/configurou no console da LANDesk. Você não tem que programar tarefas separadas. Esta tarefa é adicionada janela da ferramenta Tarefas agendadas com carimbo de hora e data.
- **Ajuda:** Abre a Central de ajuda LANDesk nos tópicos de ajuda do Data Protection.

Tópicos relacionados

"Sobre o servidor do Data Protection: Página de propriedades do servidor" na página 769

"Sobre o servidor do Data Protection: Página de conexão do banco de dados" na página 770

Distribua o software Data Protection agent para os dispositivos gerenciados

Este tópico de ajuda descreve como instalar/distribuir os softwares do agente Credant (Data Protection) necessários aos seus dispositivos gerenciados. Após instalar o agente, o dispositivo é considerado protegido (para obter mais informações, consulte "Proteção de dados da Credant" na página 761).

O agente ativa o Data Protection no dispositivo, assim com a obtenção de informações do Data Protection pelo servidor núcleo da LANDesk e a obtenção de informações instantâneas em tempo real, usadas para preencher as telas de Resumo e Inventário do console.

IMPORTANTE: Visite o site da Credant para obter instruções de instalação do agente Data Protection Recomendamos que você consulte os procedimentos de distribuição de agentes encontrados na documentação oficial da Credant. Para acessar essa documentação, vá ao site da Credant: Credant Enterprise Edition Home Page.

Tópicos relacionados

"Pré-requisitos do Data Protection" na página 763

"Use a ferramenta Data Protection" na página 764

"Exibir as informações do Data Protection no inventário" na página 765

Exibir as informações do Data Protection no inventário

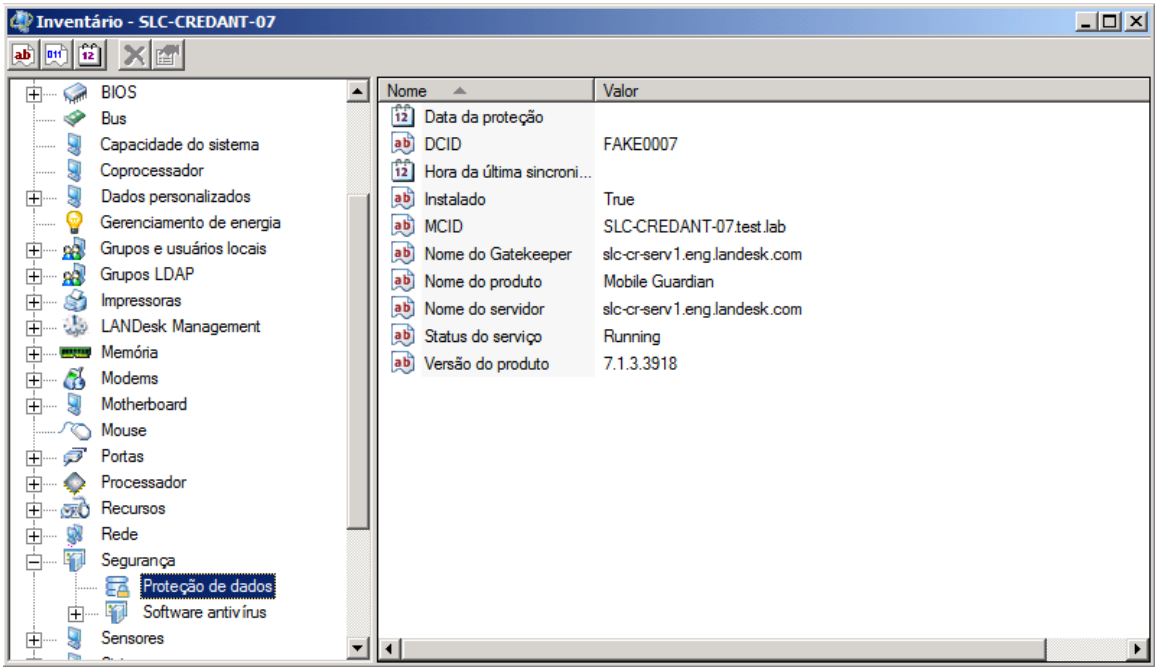
É possível visualizar as informações de proteção de dados para um dispositivo gerenciado na exibição Inventário LANDesk.

Veja informações do Data Protection no modo de exibição de Inventário.

Para ver as informações de proteção de dados para um dispositivo

1. No console, clique com o botão direito em um dispositivo gerenciado para acessar o menu de atalho.
2. Clique em **Inventário** para abrir a exibição Inventário.

3. Abra o componente **Proteção de dados** e verifique se os dados do dispositivo estão protegidos.



O componente Proteção de Dados inclui os seguintes atributos:

- **DCID:** Identifica a máquina com um código de ID exclusivo. Isso assegura que a sincronização entre o banco de dados do Data Protection e o banco de dados LDMS seja válida e precisa. O DCID será criado somente APÓS a verificação inicial completa. Talvez esteja vazio na primeira exibição, mas será preenchido depois que o agente do Data Protection for completamente verificado pelo analisador de inventário.
- **Nome do Gatekeeper:** Fornece informações específicas ao banco de dados Data Protection.
- **Instalado:** Mostra se o agente Data Protection está ou não instalado no dispositivo gerenciado.
- **Horário da última sincronização:** Mostra o horário de sincronização mais recente entre o banco de dados Data Protection e o banco de dados da LANDesk.
- **MCID:** Identificação do host definida pela configuração de agente do Data Protection. Os administradores podem utilizar essas informações para solucionar se alterarão o nome do computador, mas isso não é alterado aqui.
- **Nome do produto:** É o nome do produto Data Protection exibido no registro do dispositivo. Talvez apareça como Mobile Guardian ou Mobile Shield. Esse campo serve para fornecer informações ao administrador sobre o produto.
- **Data de proteção:** Mostra a data na qual o agente Data Protection foi instalado no dispositivo gerenciado.
- **Nome do servidor:** Mostra o nome inserido quando o servidor Data Protection foi configurado, acrescentando-o a sua rede LANDesk por meio do console.
- **Versão do produto:** O número da versão fornecida pelo arquivo de cabeçalho no serviço de instalação.

- **Status do servidor:** Mostra se o serviço de proteção de dados está em execução no dispositivo gerenciado. (**NOTA:** Essas informações foram coletadas no Gerenciador de controle de serviços do Windows.

Veja informações em tempo real do Data Protection no modo de exibição de Resumo.

Se o agente Data Protection estiver instalado em um dispositivo gerenciado, é possível visualizar a Exibição do resumo da proteção de dados por meio do menu do botão direito. Isso fornece uma visão imediata em tempo real das informações de proteção de dados atuais para o dispositivo selecionado.

Para acessar a exibição Resumo dos dados do inventário

1. Clique com o botão direito sobre o dispositivo selecionado.
2. Selecione **Resumo da proteção de dados**. (**NOTA:** Se o Data Protection não estiver instalado, essa opção estará indisponível.)
3. Visualizar as informações de proteção dos dados para esse dispositivo.

A tela de Resumo mostra as seguintes informações:

- Nome do dispositivo
- DCID
- Data da proteção
- Versão do agente
- Nome do servidor
- Gate keeper
- Nome do produto
- Última atualização

Tópicos relacionados

"Gere o relatório do Data Protection" na página 767

Gere o relatório do Data Protection

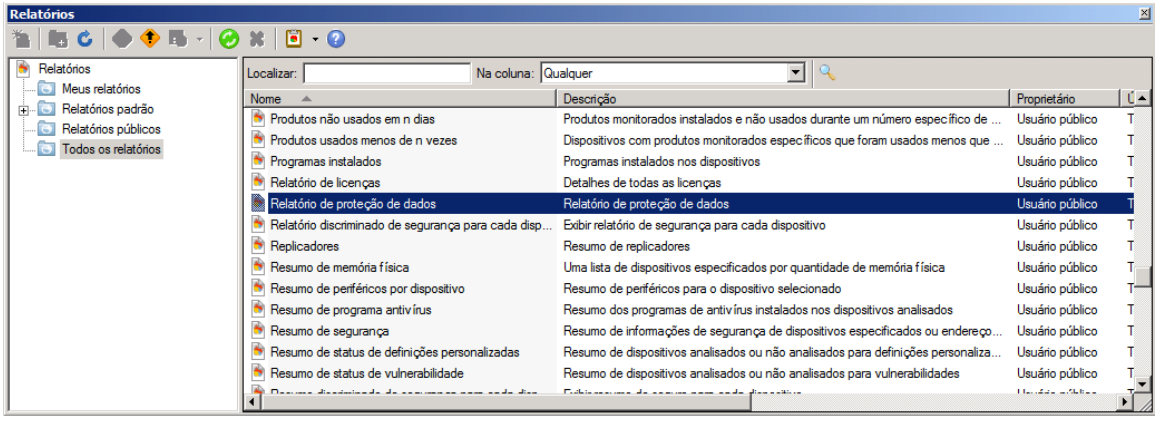
A ferramenta do LANDesk Data Protection inclui um relatório de predefinido chamado Relatório do Data Protection.

O relatório do Data Protection mostra as seguintes informações:

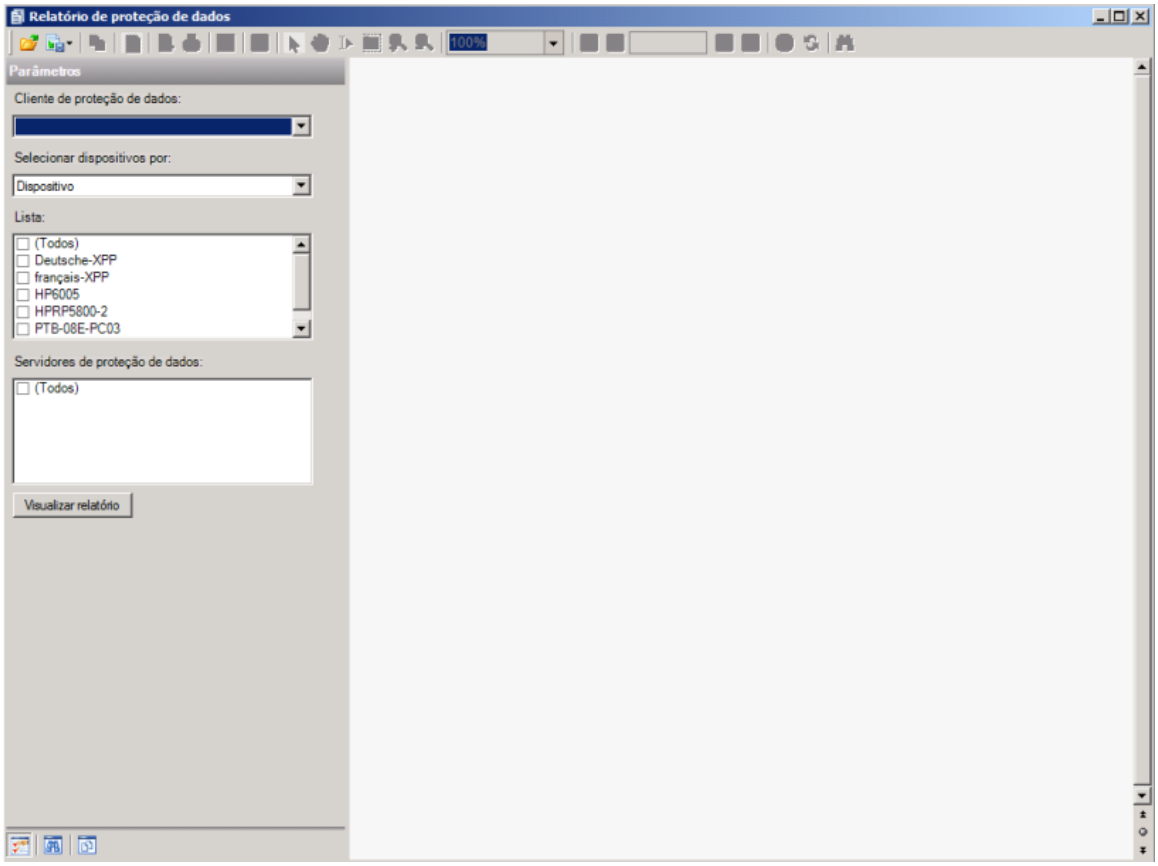
- Dispositivos protegidos
- Agentes (e versão) instalados em dispositivos
- Servidores da Credant empresarial em uso

Para gerar o relatório

1. No console da LANDesk, abra a **ferramenta Relatórios**.
2. Clique em **Todos os relatórios** e, em seguida, selecione o **Relatório do Data Protection**.


Relatórios
Relatórios
Meus relatórios
Relatórios padrão
Relatórios públicos
Todos os relatórios
Localizar:
Na coluna:
Qualquer
Nome
Descrição
Proprietário
Produtos não usados em n dias
Produtos monitorados instalados e não usados durante um número específico de ...
Produtos usados menos de n vezes
Dispositivos com produtos monitorados específicos que foram usados menos que ...
Programas instalados
Programas instalados nos dispositivos
Relatório de licenças
Detalhes de todas as licenças
Relatório de proteção de dados
Relatório de proteção de dados
Relatório discriminado de segurança para cada disp...
Exibir relatório de segurança para cada dispositivo
Replicadores
Resumo de replicadores
Resumo de memória física
Uma lista de dispositivos especificados por quantidade de memória física
Resumo de periféricos por dispositivo
Resumo de periféricos para o dispositivo selecionado
Resumo de programa antivírus
Resumo dos programas de antivírus instalados nos dispositivos analisados
Resumo de segurança
Resumo de informações de segurança de dispositivos especificados ou endereço...
Resumo de status de definições personalizadas
Resumo de dispositivos analisados ou não analisados para definições personaliza...
Resumo de status de vulnerabilidade
Resumo de dispositivos analisados ou não analisados para vulnerabilidades
Usuário público

3. Clique duas vezes no **Relatório do Data Protection** para abri-lo.



4. Especifique os parâmetros que você quer para o relatório do Data Protection.
5. Clique **Exibir relatório**.

6. Para um relato mais detalhado, clique sobre um gráfico do relatório. OU ir para a segunda página do relatório para ver a visualização detalhada do texto.

Tópicos relacionados

"Exibir as informações do Data Protection no inventário" na página 765

Sobre o servidor do Data Protection: Página de propriedades do servidor

Use este diálogo para adicionar um servidor do Data Protection (que já foi instalado e foi configurado de acordo com requisitos de servidor da Credant e instruções) a seu ambiente de rede da LANDesk. O servidor do Data Protection fornece informações sobre a integridade de dados de seus dispositivos gerenciados ao servidor núcleo da LANDesk onde você pode exibi-lo no modo de exibição do Inventário e através da ferramenta de Relatórios.

Você pode ter um ou mais servidores do Data Protection.

O servidor configurado cria a conexão entre os bancos de dados do Data Protection e do núcleo da LANDesk, o que permite que você sincronize dados entre os servidores e os dispositivos gerenciados "protegidos" em sua rede. O servidor então preenche o banco de dados núcleo da LANDesk com informações que podem ser exibidas no modo de exibição de Inventário e no modo de exibição de Resumo do Data Protection (atualizações em tempo real).

NOTA: TODOS os servidores do Data Protection são analisados
Todos os servidores relacionados do Data Protection (configurados/adicionados) serão analisados e usados para preencher o banco de dados do núcleo da LANDesk. Você não pode especificar um único servidor. Você não pode sincronizar um por vez. Independentemente de quantos servidores você tem na lista, todos serão sincronizado pela tarefa agendada.

Essa página contém as seguintes opções:

- **Nome do servidor:** Identifica o servidor do Data Protection que você quer adicionar. Você pode inserir um endereço válido de IP ou nome do host de domínio totalmente qualificado para o servidor desejado.
- **Descrição:** Insira qualquer informação que você deseja para distinguir este servidor de qualquer outro que você talvez adicione.
- **Nome do proxy da diretiva:** Usado para uma instalação do agente Credant.
- **Porta:** Especifica o número da porta utilizada pelo servidor do Data Protection para permitir a sincronização de dados com o banco de dados do núcleo da LANDesk.
- **URL do servidor do dispositivo:** Especifica o endereço da Web usado para iniciar o console Web nativo da Credant.
- **Teste:** Verifique se as informações do servidor que você inseriu representa um servidor válido em sua rede.
- **Cancelar teste:** Encerra o processo de verificação de servidor.
- **Salvar:** Salva as alterações e fecha a caixa de diálogo.
- **Cancelar:** Fecha a caixa de diálogo sem salvar as alterações.

Tópicos relacionados

"Sobre o servidor do Data Protection: Página de conexão do banco de dados" na página 770

"Proteção de dados da Credant" na página 761

Sobre o servidor do Data Protection: Página de conexão do banco de dados

Use esta página para configurar uma conexão à banco de dados usada pelo servidor do Data Protection adicionado. O banco de dados do Data Protection reúne informações sobre tipos de dados que você especifica para seus dispositivos gerenciados e transmite essas informações ao banco de dados núcleo da LANDesk.

NOTA: Informações inseridas resolvidas em tempo real
As informações inseridas nos campos nesta página serão resolvidos em tempo real pelo servidor núcleo da LANDesk. Você será notificado se as informações são válidas ou não.

Essa página contém as seguintes opções:

- **Servidor do banco de dados:** O nome do servidor hospedando o banco de dados do Data Protection.
- **Nome do banco de dados:** O nome do banco de dados do Data Protection.
- **Nome de usuário:** Insira um nome de usuário válido para o servidor do Data Protection que você quer adicionar (configurar).
- **Senha:** Insira a senha para o usuário especificado acima.
- **Teste:** Verifique se as informações do servidor que você inseriu representa um servidor válido em sua rede. (**NOTA:** O teste começará automaticamente se você pausar durante a inserção no servidor do banco de dados, nome, nomes de usuário ou senha. Em outras palavras, você necessariamente não tem que clicar no botão Testar).
- **Cancelar teste:** Encerra o processo de verificação de servidor.
- **Salvar:** Salva as alterações e fecha a caixa de diálogo.
- **Cancelar:** Fecha a caixa de diálogo sem salvar as alterações.

Tópicos relacionados

"Sobre o servidor do Data Protection: Página de propriedades do servidor" na página 769

"Proteção de dados da Credant" na página 761

Gerenciador de link do LaunchPad

Sobre o LaunchPad

O LaunchPad LANDesk fornece um local conhecido para os usuários encontrarem seus aplicativos virtuais e físicos e URLs. Reduze chamadas ao escritório de ajuda que envolve a instalação de aplicativos ou ícones faltantes do desktop. O LaunchPad fornece uma lista de aplicativos conhecidos a um grupo conhecido de usuários (ou dispositivos). Lhe impede ir de sistema a sistema (manualmente ou usando o controle remoto) para consertar problemas específicos de aplicativo.

O LaunchPad impede usuários excluir ícones ou quebrar aplicativos instalados. Atualiza automaticamente desktops de usuários finais com novos aplicativos para grupos designados. Os usuários poderão fazer login em qualquer computador e terão seus links extraídos ao LaunchPad nessa máquina.

Você pode criar um link de pacote de distribuição que liga diretamente a instalação de um aplicativo com sua execução (também conhecido como link Just In Time, ou JIT, link). Uma definição do link JIT é criada no console selecionando Pacote de distribuição como o tipo de link, e associando um pacote de distribuição de software com o link.

Quando um link JIT aparecer no LaunchPad e for aberto por um usuário, o software LANDesk do cliente do tentará distribuir o pacote de distribuição de software associado antes que o aplicativo alvo seja executado. Observe que a diferença dos alvos de links de tipo "executáveis", alvos de links JIT devem ser eles mesmos arquivos executáveis; o LaunchPad não determina associações de arquivos para links JIT como faz com links ordinários.

Se a distribuição do pacote é bem sucedida, o executável alvo será iniciado e o link será marcado para que a distribuição seja pulada e o executável seja iniciado diretamente.

Já que links JIT estão desenhados para ocultar o processo de instalação do usuário final, pacotes de distribuição de software que atrapalham o fluxo de trabalho normal de um usuário, como aqueles que requerem uma reinicialização, significante digitação do usuário, ou um tempo incomum longo para instalar não devem estar associados com links JIT. Estes tipos de pacotes de distribuição de software devem ser distribuídos usando o Portal de distribuição de software LANDesk (que permite ao usuário controlar o tempo e a maneira de distribuir o pacote) ou uma distribuição por envio padrão durante horas de inatividade .

Links de LaunchPad que não forem JIT não serão exibidos na janela LaunchPad se o alvo não for localizado, então você pode criar um link ordinário para um executável ou arquivo que será instalado mais tarde. O ícone do link não aparecerá na janela LaunchPad até que o alvo tenha sido criado por uns destes métodos alternativos.

Para abrir o LaunchPad em Management Suite

1. Clique em **Ferramentas > Distribuição > Gerencidor de link do LaunchPad**.

Colunas

- **Nome:** O nome do link como definido nas **Propriedades do link**.
- **Descrição:** A descrição do link como definida nas **Propriedades do link**.
- **Local:** Onde está localizado o link (LaunchPad, desktop, ou menu Iniciar).
- **Categoria:** A classificação do link. Exemplos incluem aplicativos, utilitários ou links web. Você pode criar categorias para atender às necessidades da sua empresa. Os usuários finais verão uma interface

exibindo cada categoria em sua própria fileira.

- **Caminho:** O local do executável do link.

Adicionando links ao LaunchPad

Itens são adicionados ao LaunchPad como links. O links (exibidos como ícones no LaunchPad) podem representar aplicativos, utilitários, links para páginas web e etc. Antes que os links possam ser exibidos, as seguintes instruções devem ser concluídas.

Ao distribuir links de LaunchPad a um computador cliente, os links não aparecerão no computador (Desktop, menu de Início ou janela LaunchPad) até que o programa de sincronização da diretiva de distribuição de software LANDesk seja executado no computador. Quando for invocado, o programa de sincronização da diretiva contatará o núcleo LANDesk, solicitará e fará o download qualquer atualização, incluindo novos links LaunchPad.

Geralmente, o Programa de sincronização da diretiva é agendado para executar periodicamente nos computadores cliente. Os administradores podem também executar a sincronização de diretiva quando quiser usando os procedimentos abaixo. Outra alternativa é permitir que os usuários invoquem o programa de sincronização da diretiva por eles mesmos, usando um link LaunchPad, como descrito em “Para configurar um link do programa de sincronização da diretiva nos computadores cliente” abaixo.

Para executar sincronização de diretivas (policy.sync.exe) uma vez em um computador cliente,

1. Execute o seguinte comando:

Para um OS de 32 bit:

```
"%ProgramFiles%\LANDesk\Shared Files\httpclient.exe" "http://localhost:9595/policy.cgi.exe?action=start"
```

Para um OS de 64 bit:

```
"%ProgramFiles(x86)%\LANDesk\Shared Files\httpclient.exe"
"http://localhost:9595/policy.cgi.exe?action=start"
```

Para forçar uma sincronização em um cliente a partir do núcleo

1. Abra o console do Management Suite no núcleo.
2. Clique em **Ferramentas > Distribuição > Gerenciar scripts**.
3. No painel à esquerda, clique em **Todos os scripts**.
4. Clique com o botão direito no script "Package Sync" e clique em **Agendar**.
5. Na tela de rede, arraste o cliente que deseja sincronizar à tarefa Package Sync.
6. Clique com o botão direito do mouse na tarefa Package Sync e clique em **Propriedades**.
7. Clique no painel **Agendar tarefa**, selecione **Iniciar agora** e **Todos os dispositivos** na caixa **Agendar estes dispositivos**.
8. Clique em **Salvar**. Um script executará invocando a sincronização de diretiva no cliente alvo. Como você selecionou todos os dispositivos, se quiser executar a tarefa novamente no futuro, simplesmente clique em **Iniciar agora** e depois em **Salvar** na página **Agendar tarefa** para executar o script novamente.

NOTA: Lembre-se que cada computador com este script dirigido tentará contatar o núcleo e atualizar seus diretivas. Se enviado a um número grande de computadores, isto pode causar problemas ao servidor núcleo.

Para configurar um link do programa de sincronização da diretiva em computadores cliente

1. No console LANDesk, crie um link executável do LaunchPad com a etiqueta “Atualizar” que aponta para “"%ProgramFiles%\LANDesk\Shared Files\httpclient.exe" "http://localhost:9595/policy.cgi.exe?action=start".
2. Clique com o botão direito do mouse no link e clique em **Agendar**.
3. Na tela de rede, arraste o cliente que deseja distribuir à tarefa do link.
4. Clique com o botão direito do mouse na tarefa e clique em **Propriedades**.
5. Clique no painel **Agendar tarefa** e clique em **Iniciar agora**. O link aparecerá no computador cliente a próxima vez que a sincronização de diretiva ocorrer.

Para adicionar links ao LaunchPad

1. Se o LaunchPad não abrir, clique em **Ferramentas > Distribuição > Gerenciador de links do LaunchPad**.
2. Na barra de ferramentas do LaunchPad, clique em **Adicionar novo link**.
3. Clique nas páginas no painel esquerdo e preencha os campos no painel direito. Consulte as informações adicionais abaixo para os campos nestas páginas. Ao terminar, clique em **Salvar**.

Gerenciamento de energia

Visão geral do Gerenciamento de energia do LANDesk®

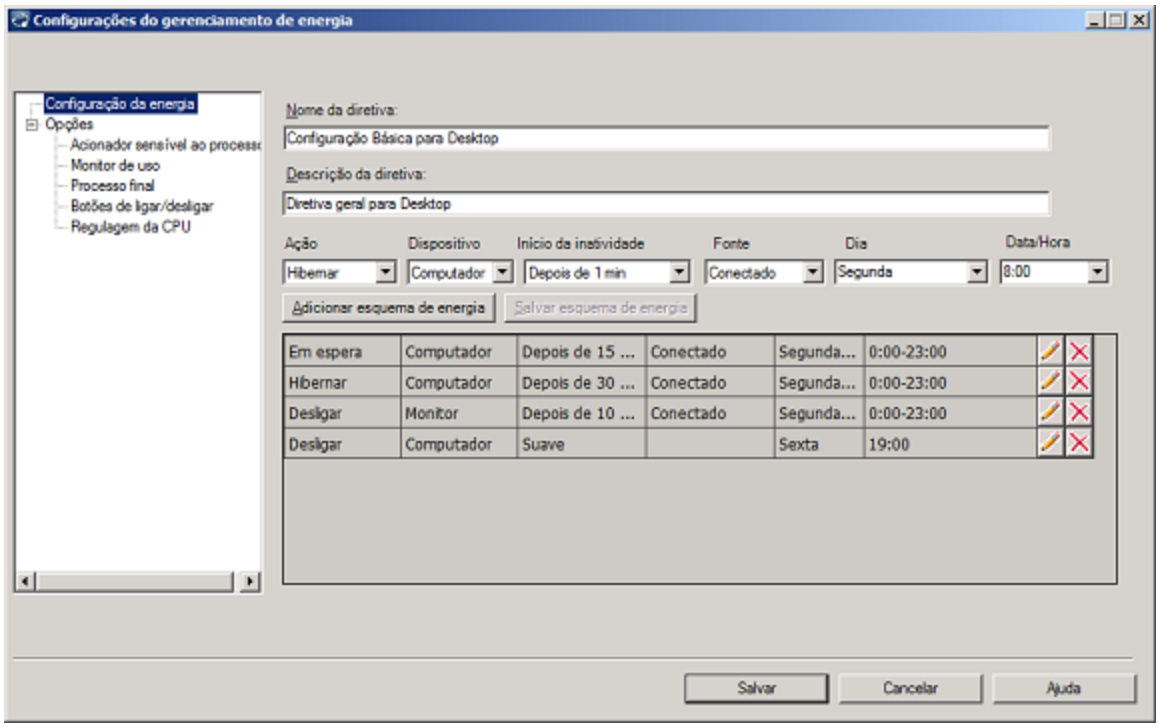
A ferramenta de gerenciamento de energia do LANDesk permite monitorar a utilização da energia dos computadores gerenciados a partir de um local central. É possível criar e distribuir com facilidade diretivas de gerenciamento de energia e gerar relatórios para avaliar a economia financeira e de energia. Controle as condições de espera, hibernação ou desligamento de computadores e monitores.

O Gerenciamento de energia inclui um recurso que permite que o usuário evite ações específicas de gerenciamento de energia, como um desligamento forçado, pelo uso de uma interface de usuário no cliente. A ação evitada ocorrerá da próxima vez que a diretiva for executada ou atualizada naquele computador.

Como funciona

O agente LANDesk distribuído a todos os dispositivos gerenciados inclui uma opção de gerenciamento de energia. Ao escolher distribuir uma diretiva de gerenciamento de energia em um dispositivo, que é ativado por parte do agente.

Defina diretivas com base nas necessidades específicas dos diferentes tipos de dispositivos gerenciados. Em seguida, você pode implementar as diretivas nos grupos de dispositivos da empresa. Por exemplo, você definiria uma diretiva para servidores que precisam estar em execução continuamente, e uma diretiva diferente para desktops que normalmente não são usados a noite e nos finais de semana.



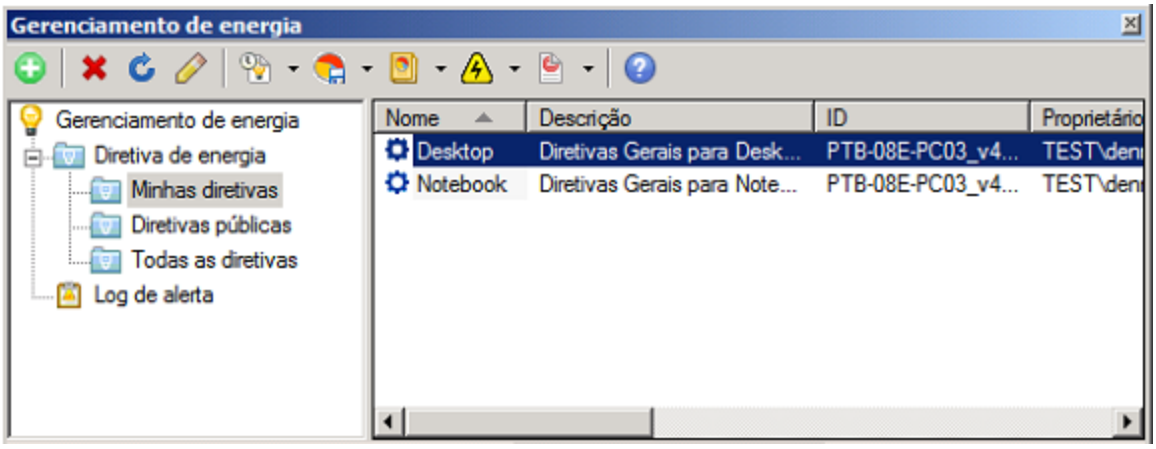
Cada diretiva contém um ou mais esquemas de energia, que são regras específicas relativas a ações relacionadas com energia. Cada esquema se aplica a um tipo de dispositivos durante um período especificado. Por exemplo, você pode

- Aplicar regras de espera ou de hibernação que são válidas para um desktop ou laptop durante horas de uso regular
- Definir os esquemas de monitores para desligar após um período de inatividade
- Define esquemas para ligar dispositivos automaticamente em determinadas horas

Se um usuário está trabalhando em um computador, em um horário que a diretiva normalmente o desligaria, uma interface de cliente notifica o usuário, que pode adiar o encerramento conforme necessário.

Botões da barra de ferramentas do gerenciamento de energia

A ferramenta de gerenciamento de energia inclui um conjunto de botões de ferramenta que possibilitam completar várias tarefas de gerenciamento de energia.



- **Novo:** Clique para criar uma nova diretiva de gerenciamento de energia.
- **Excluir:** Exclui a diretiva de gerenciamento de energia selecionada.
- **Atualizar:** Atualiza os itens exibidos no painel esquerdo.
- **Propriedades:** Exibe as propriedades da diretiva de gerenciamento de energia selecionada.
- **Agendar:** Clique para agendar a distribuição da diretiva de gerenciamento de energia selecionada.
- **Relatórios:** Clique para executar um relatório que estima as economias de energia e custos obtidas pela distribuição da diretiva de gerenciamento de energia selecionada para o grupo de dispositivos especificado. Você também pode executar um relatório que mostra a economia de energia e dinheiro durante um intervalo de tempo específico.
- **Dados históricos:** Clique para obter informações de uso do cliente para uma estimativa mais precisa do consumo de energia.
- **Personalizar:** Permite personalizar as configurações que definem a utilização geral da energia de acordo com fabricantes e modelos de computadores específicos.
- **Gerenciamento de aplicativos:** Permite o gerenciamento de processos que podem estar em execução quando uma diretiva de energia é aplicada.

Criação de uma diretiva de gerenciamento de energia

O Gerenciamento de energia usa o gerenciamento com base em diretivas para enviar instruções de espera, hibernação, desligamento e ativamento dos computadores gerenciados. Crie diretivas de gerenciamento de energia para controlar computadores e grupos de computadores específicos.

Para criar uma diretiva de gerenciamento de energia

1. Clique em **Ferramentas > Gerenciamento de energia > Gerenciamento de energia**.
2. Clique em uma pasta de diretivas no modo de exibição de árvore.
3. Clique no botão **Nova** na barra de ferramentas.
4. Digite um nome e descrição para a diretiva.
5. Adicione pelo menos um esquema de energia para a diretiva. Selecionar as configurações das seis listas (**Ação**, **Dispositivo**, **Acionador de inatividade**, **Origem**, **Dia** e **Hora**) e clique em **Adicionar esquema de energia**.

   Você pode adicionar vários esquemas de energia, conforme necessário. Para remover um esquema de alimentação de uma diretiva, clique no botão **Excluir** ( ) ao lado do esquema.
6. Expanda as **Opções** na coluna à esquerda. Selecione as configurações nas páginas das seis opções.
7. Quando todas as opções estiverem definidas, clique em **Salvar**.

Clique aqui para ver as descrições das opções do esquema de energia e da diretiva de energia

Opções do esquema de energia

- **Ação:** Selecione a ação a executar no computador gerenciado — hibernar, espera, ativação, desligamento.
- **Dispositivo:** Selecione o dispositivo onde a ação será executada (por exemplo, computador).
- **Indicador de inatividade:** Selecione o intervalo de tempo a decorrer antes da ação ser disparada (1 minuto a 5 horas ou nunca). Observação: Se você selecionar **Desligar** na lista **Ação**, o título da lista muda de **Acionador de inatividade** para **Tipo de desligamento** (forçado ou programado).
- **Origem:** Selecione a origem da energia que o dispositivo está utilizando (conectado à tomada, à bateria ou a ambos).
- **Dia:** Selecione o dia ou os dias da semana para executar a ação.
- **Hora:** Selecione a hora ou as horas do dia para executar a ação.

Opções da diretiva de energia

- **Opções:** Desative a proteção de tela, Ative o acionamento local, Adie o desligamento, Monitore.
- **Disparo sensível a processo** Use esta página para adiar a diretiva de energia se qualquer um dos processos relacionados for detectado. A diretiva continuará se nenhuma outra diretiva for detectada após os minutos especificados. Para adicionar processos a esta lista, use o botão da **listaAcionadores sensíveis a processo** da barra de ferramentas.
- **Monitor de uso:** Habilite esta opção para aplicar a diretiva de energia se as condições especificadas no diálogo forem satisfeitas. Condições que podem ser especificadas são o uso da CPU e tráfego da rede. Se uma ou ambas atingirem a porcentagem especificada abaixo do máximo, a diretiva de energia será imposta.

- **Encerrar processo:** Ative esta opção para encerrar os processos na lista durante o encerramento. Para adicionar os processos a esta lista, use o botão **Lista processos para encerrar** na barra de ferramentas.
- **Botões de energia:** Ative esta opção para configurar as ações resultantes quando um usuário pressionar o interruptor liga/desliga de um dispositivo gerenciado. Selecione a ação a ser executada para cada opção quando a máquina estiver ligada na tomada ou na bateria. Para cada situação, as ações que você pode escolher são **Fazer nada**, entrar em **Modo de espera**, **Hibernar** ou **Desligar**.
- **Controle da CPU:** Ative esta opção para configurar o Controle da CPU (restringindo os níveis de energia da CPU) de uma diretiva de energia distribuída. Selecione um nível de desempenho quando a máquina é ligada na tomada ou na bateria. As opções de desempenho são **Mais elevado** (mínimo 100, máximo 100), **Adaptativo** (mínimo 5, máximo 100), **Baixo** (mínimo 5, máximo 50) ou **Mais baixo** (mínimo 5, máximo 33).

Usar a ação Ligar em Wake-on-LAN

O gerenciamento de energia usa a tecnologia WOL (Wake on LAN), ou Intel vPro wake up, para ligar um computador remotamente a fim de executar tarefas agendadas. Para que o Gerenciamento de energia use a função WOL, os adaptadores de rede dos computadores gerenciados devem estar configurados corretamente para dar suporte à WOL.

O Gerenciamento de energia não pode ajustar ou configurar a função WOL dos adaptadores de rede. Se a função WOL do adaptador de rede de um computador não estiver ativada, uma diretiva de gerenciamento de energia que inclua uma ação de "ativação" em seu esquema de energia falhará naquele computador. Atualmente o Gerenciamento de energia não inclui uma forma de monitorar se a função WOL do adaptador de rede está ativada.

Usar a Hibernação no Windows 2000 e Windows XP SP2

O Gerenciamento de energia não pode habilitar a função hibernar automaticamente em computadores com Windows 2000 e no Windows XP SP2. Usuários dos computadores gerenciados devem habilitar manualmente a função Hibernar através do Painel de controle.

1. No Painel de controle, clique duas vezes em **Opções de energia**.
2. Na caixa de diálogo **Propriedades das Opções de energia** clique na guia **Hibernar** .
3. Marque a caixa de seleção **Ativar hibernação** e clique em **OK**.

Distribuição de uma diretiva de gerenciamento de energia

Depois de criar uma diretiva, você deve agendá-la para executar em um dispositivo ou grupo de dispositivos gerenciados. Depois de concluir a tarefa com êxito, o agente da LANDesk presente nos dispositivos-alvo inclui a diretiva de energia e usa os esquema de energia na diretiva.

Para distribuir uma diretiva de gerenciamento de energia

1. Clique em **Ferramentas > Gerenciamento de energia > Gerenciamento de energia**.
2. Clique em uma pasta de diretivas no modo de exibição de árvore e selecione a diretiva.
3. Clique no botão **Agenda** na barra de ferramentas e selecione **Agendar diretiva**.

   A ferramenta **Tarefas agendadas** é iniciada quando a diretiva de energia é selecionada.
4. Arraste um dispositivo ou grupo da tela de rede para a diretiva.

5. Clique com o botão direito na diretiva e em **Iniciar agora**.
6. Para iniciar a tarefa em outro momento, selecione a diretiva, clique no botão **Propriedades** da barra de ferramentas e especifique a hora para iniciar a tarefa da diretiva.

Os painéis de status de tarefas mostram quais dispositivos concluíram a tarefa com êxito. Se a tarefa não pode ser concluída em todos os dispositivos, o motivo da falha é mostrado.

NOTA: O agente da LANDesk de dispositivos alvos devem ter o gerenciamento de energia ativado para que uma diretiva de energia funcione. Se você implementar uma diretiva e receber um mensagem de erro que a tarefa da diretiva não pode ser iniciada em um dispositivo, certifique-se de que o gerenciamento de energia esta ativado no agente do dispositivo.

Remove uma diretiva de gerenciamento de energia

Você pode excluir diretivas de gerenciamento de energia de todos os dispositivos gerenciados ou de grupos de dispositivos. Isto é feito criando uma tarefa agendada que é aplicada a todos os dispositivos. Depois de concluir a tarefa com êxito, o agente da LANDesk presente nos dispositivos-alvo não mais incluirá a diretiva de energia.

Para remover uma diretiva de gerenciamento de energia

1. Clique em **Ferramentas > Gerenciamento de energia > Gerenciamento de energia**.
2. Clique no botão **Agenda** na barra de ferramentas e selecione a opção **Desligar gerenciamento de energia**.

   Se você selecionar a opção global, o gerenciamento de energia é removido de todos os dispositivos gerenciados.

   Se você selecionar a opção grupo, selecione o grupo de dispositivos ou consulta dos qual você deseja remover o gerenciamento de energia e clique em **OK**.
3. Na ferramenta Tarefas agendadas, clique com o botão direito em **Desligar gerenciamento de energia** e clique em **Iniciar agora**.
4. Para iniciar a tarefa em outro momento, selecione a tarefa, clique no botão **Propriedades** na barra de ferramentas e especifique a hora para iniciar a tarefa de remoção.

Os painéis de status de tarefas mostram quais dispositivos concluíram a tarefa com êxito. Se a tarefa não pode ser concluída em todos os dispositivos, o motivo da falha é mostrado.

Agendar ativação remota

O Gerenciamento de energia agenda um comando "ligar" no BIOS do dispositivo. Se o BIOS não consegue agendar eventos a acionamento, ou não consegue agendá-los através do Windows, o evento "ligar" não será agendado. Quando isso acontecer, existem várias formas de resolver o problema:

- Habilitar eventos 'plug and play' no BIOS
- Ativar eventos no BIOS
- Atualizar o BIOS

Alguns BIOS não suportam esta funcionalidade. Nessa situação, uma tarefa agendada de Wake on LAN pode ser usada para ligar dispositivos em um momento específico.

Se um dispositivo gerenciado é configurado para usar WOL (Wake on LAN) ou o Intel vPro 'wake up', você pode agendar um 'despertador' remoto para ligar o dispositivo em uma hora específica. Este recurso aciona dispositivos em modo de espera ou hibernação e liga os dispositivos desligados.

Se o WOL e o Intel Vpro wake up estiverem ativados, o recurso Intel Vpro é executado primeiro e WOL é executado em seguida.

Para agendar uma ativação remota

1. Clique em **Ferramentas > Gerenciamento de energia > Gerenciamento de energia**.
2. Clique no botão **Agenda** na barra de ferramentas e selecione **Agendar ativação remota**.

   A ferramenta **Tarefas agendadas** é iniciada com a tarefa selecionada.
3. Arraste um dispositivo ou grupo de dispositivos da tela de rede para a tarefa.
4. Clique com o botão direito na diretiva e em **Iniciar agora**.
5. Para iniciar a tarefa outro hora, selecione a tarefa, clique no botão **Propriedades** na barra de ferramentas e especifique a hora para iniciar a tarefa.

Os painéis de status de tarefas mostram quais dispositivos concluíram a tarefa com êxito. Se a tarefa não pode ser concluída em todos os dispositivos, o motivo da falha é mostrado.

Gerenciar aplicativos em conflito com as diretivas de energia

Aplicativos em execução em dispositivos gerenciados podem entrar em conflito com as diretivas de gerenciamento de energia criadas. Alguns aplicativos devem ser autorizados a continuar a funcionar mesmo se a diretiva tiver um comando de desligamento para o dispositivo. Outros aplicativos não devem interferir com a diretiva e devem ser encerrados como parte do processo de desligamento.

O log de alerta do gerenciamento de energia ajuda a identificar quais processos em execução nos dispositivos gerenciados podem entrar em conflito com as políticas de energia. Estes conflitos são registrados com o nome do dispositivo, hora e o nome do processo. Reveja essas entradas de log para determinar quais aplicativos geram conflitos.

O botão **Gerenciamento de aplicativos** ( ) na barra de ferramentas de gerenciamento de energia inclui três opções que permitem o gerenciamento de possíveis conflitos com aplicativos:

- Identificar acionadores sensíveis a processo: Os processos incluídos nesta lista serão autorizados a funcionar mesmo que a diretiva de energia tenha um comando de desligamento. A diretiva de energia irá esperar até que os processos sejam encerrados e continuará a aplicar a diretiva.
- Identificar processos para serem encerrados no desligamento: Os processos incluídos nesta lista podem interferir com a diretiva de energia, provocando um estado de "insônia" (incapacidade do dispositivo de desligar ou hibernar). Se estes processos estão em execução, a diretiva de energia será encerrada para que eles continuem.
- **Identificar processos para ignorar**: Os processos incluídos nesta lista não precisam de atenção da diretiva de energia e nem precisam ser incluídos nos logs de alerta.

Instruções para usar estas opções são encontradas nos seguintes tópicos:

"Configurar aplicativos que não devem ser desligados" na página 780

"Configurar aplicativos que devem ser desligados" na página 780

"Configurar aplicativos para serem ignorados nos logs de alerta" na página 781

Configurar aplicativos que não devem ser desligados

Use o botão **Identificar disparos sensíveis a processo** da barra de ferramentas para observar o processo de qualquer programa importante e aguardar sua conclusão antes de aplicar as diretivas de energia.

Em alguns ambientes, os programas precisam ser executados por um período prolongado. Por exemplo, o processo do Management Suite Patch pode ser curto ou longo na instalação de patches. O período necessário para o dispositivo gerenciado ser ativado é desconhecido quando se trata de distribuição de patches. Outros programas podem ter parâmetros semelhantes que precisam ser ininterruptos em certos ambientes.

Para identificar aplicativos que não deve ser desligados

1. Clique em **Ferramentas > Gerenciamento de energia > Gerenciamento de energia**.
2. Clique no botão **Gerenciamento de aplicativos** na barra de ferramentas e selecione **Identificar acionadores sensíveis a processo**.
3. Adicione, modifique ou exclua nomes de processos na lista.
4. Quando a lista estiver completa, clique em **OK**.

NOTA: A lista que você criar aqui, só se aplica a um dispositivo gerenciado se você ativou a opção acionador sensível ao processo na diretiva de gerenciamento de energia do dispositivo.

Clique aqui para obter descrições das opções na caixa de diálogo **lista de Acionadores sensíveis a processo**

- **Adicionar:** Adiciona um processo que é um .exe conhecido o qual precisa retardar as diretivas de energia.
- **Importar:** Adiciona um processo das informações coletadas dos computadores clientes usando informações de **Dados históricos**. Isto inclui processos que estão listados no log de alerta do gerenciamento de energia.
- **Excluir:** Remove o processo selecionado dessa lista.
- **Modificar:** Selecione este botão para mudar o nome do arquivo .exe.
- **Todos:** Seleciona todos os processos na lista.
- **Nenhum:** Limpa todos os processos da lista.

Configurar aplicativos que devem ser desligados

Use o botão **Identificar processos para serem encerrados no desligamento** da barra de ferramentas para interromper processos que podem atrasar uma opção da diretiva de energia. Alguns processos fazem com que o computador não siga os parâmetros de diretivas de energia configurados. Esse mesmo processo afeta alguns ou muitos dos computadores que seguem a diretiva. O gerenciamento de energia encerra os processos que impedem o dispositivo de hibernar ou desligar.

Para identificar aplicativos que devem ser encerrados como parte do desligamento

1. Clique em **Ferramentas > Gerenciamento de energia > Gerenciamento de energia**.
2. Clique no botão **Gerenciamento de aplicativos** na barra de ferramentas e selecione **Identificar processos para serem encerrados no desligamento**.
3. Adicione, modifique ou exclua nomes de processos na lista.
4. Quando a lista estiver completa, clique em **OK**.

NOTA: A lista que você criar aqui, só se aplica a um dispositivo gerenciado se você ativou a opção lista de fim de processo na diretiva de gerenciamento de energia do dispositivo.

Clique aqui para obter descrições das opções na caixa de diálogo **Lista processos para encerrar**

- **Adicionar:** Adiciona um processo que é um .exe conhecido o qual precisa ser encerrado.
- **Importar:** Adiciona um processo a partir das informações coletadas dos computadores de clientes usando informações de **Dados históricos**. Isto inclui processos que estão listados no log de alerta do gerenciamento de energia.
- **Excluir:** Remove o processo selecionado dessa lista.
- **Modificar:** Selecione este botão para mudar o nome do arquivo .exe.
- **Todos:** Seleciona todos os processos na lista.
- **Nenhum:** Limpa todos os processos da lista.

Configurar aplicativos para serem ignorados nos logs de alerta

Use o botão **Identificar processos para ignorar nos logs de exceção** na barra de ferramentas para designar processos que não precisam de atenção da diretiva de energia. Adicionar processos a esta lista pode reduzir o tamanho dos arquivos de log relacionados com o gerenciamento de energia, o que ajudará você a se concentrar nos aplicativos que são importantes para o monitoramento de problemas com o gerenciamento de energia.

Para identificar os aplicativos que podem ser ignorados em logs de alerta

1. Clique em **Ferramentas > Gerenciamento de energia > Gerenciamento de energia**.
2. Clique no botão **Gerenciamento de aplicativos** na barra de ferramentas e selecione **Identificar processos para ignorar nos logs de exceção**.
3. Adicione, modifique ou exclua nomes de processos na lista.
4. Quando a lista estiver completa, clique em **OK**.

Clique aqui para obter descrições das opções na caixa de diálogo **Processos para ignorar**

- **Adicionar:** Adiciona um processo que é um arquivo .exe conhecido que pode ser ignorado.
- **Importar:** Adiciona um processo a partir das informações coletadas dos computadores de clientes usando informações de **Dados históricos**. Isto inclui processos que estão listados no log de alerta do gerenciamento de energia.
- **Excluir:** Remove o processo selecionado dessa lista.

- **Modificar:** Selecione este botão para mudar o nome do arquivo .exe.

Exibir relatórios de Gerenciamento de energia

A ferramenta Gerenciamento de energia permite que você emita e veja relatórios de energia, redução de custos e histórico. Os relatórios são feitos de cálculos compostos de economia financeira ou de potência elétrica. Eles são baseados nos custos estimados de potência e em uma média de uso nos computadores selecionados que você associou a um relatório.

Há dois tipos de relatórios de economia:

- **Potência**: compara o número de kWh (quilowatt) usado quando as diretivas de gerenciamento de energia estão em vigor com o valor usado se não houver uma diretiva de gerenciamento de energia estiver em efeito.
- **Economia**: cria uma estimativa da economia alcançada quando as diretivas de gerenciamento de energia são aplicadas.

A economia pode ser calculada por dia, semana, mês ou ano. Se você tiver dados históricos, você pode executar relatórios históricos dos mesmos tipos.

Como os relatórios são criados

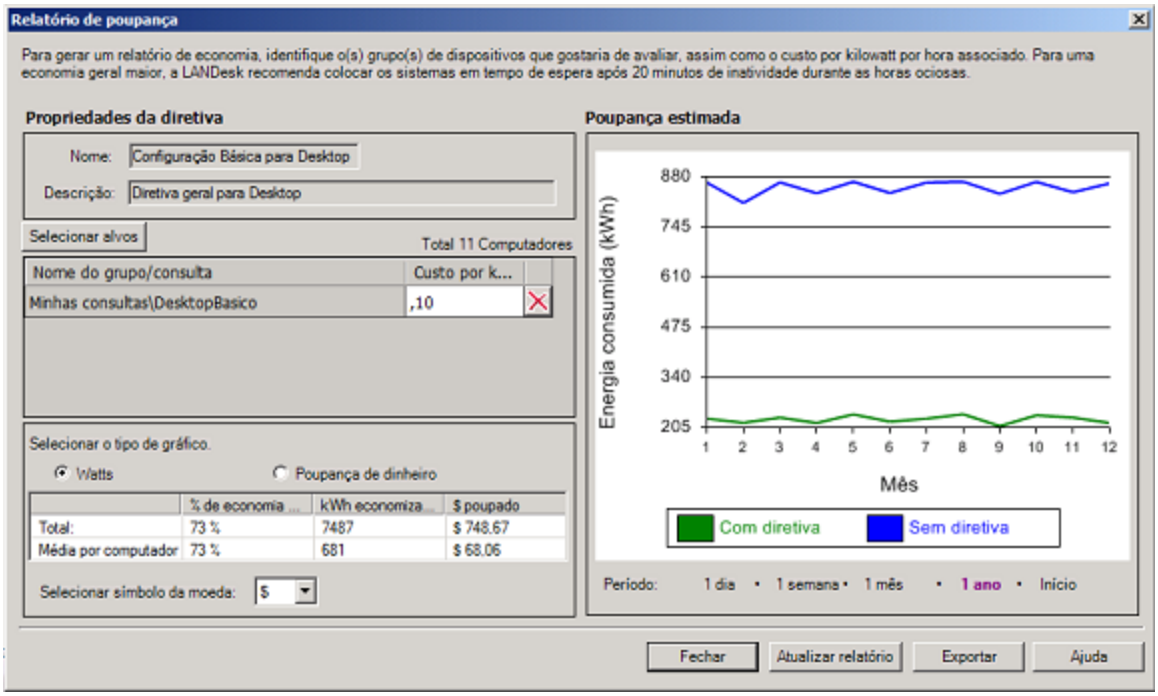
Os processos de gerenciamento de energia em dispositivos gerenciados rastreiam o tempo que cada dispositivo está em uso de forma ativa. Os relatórios são criados a partir de um arquivo de XML que reúne as informações de uso e calcula uma média do tempo que os computadores estão em uso.

Todas as vezes que executar um relatório, você selecionará dispositivos ou grupos de dispositivos. Em seguida, o relatório reúne dados para esses dispositivos e apresenta um resumo do uso. As horas de uso são multiplicados pela potência média para o tipo de dispositivo (relatórios de potência elétrica) ou o custo estimado da economia por manter o dispositivo desligado (relatórios de economia financeira).

Os elementos a seguir contribuem para os cálculos nos relatórios. Você pode modificar qualquer um desses elementos para criar relatórios mais precisos para a sua situação.

- **Custo por kWh**: uma média padrão é usada como padrão. Se você conhece o custo real por kWh da sua conta de eletricidade, alterar este número.
- **Configurações personalizadas de potência elétrica**: por padrão, os relatórios usam a média das configurações de potência elétrica para desktops e laptops. Se você deseja usar os dados mais específicos, você pode usar os dados para determinados fabricantes e modelos.
- **Dados de uso do cliente**: por padrão, a média de uso diária do cliente é usada para os cálculos. Se você deseja usar dados mais específicos, você pode aplicar dados históricos extraídos os seus dispositivos gerenciados para cálculos de relatório.

Ao executar um relatório de economia, você usa a caixa de diálogo a seguir para selecionar opções e visualizar os resultados.



Executar um relatório de gestão de energia

Use o botão **Relatórios** na barra de ferramentas de gerenciamento de energia para executar relatórios de economia e históricos.

NOTA: Os relatórios requerem que você primeiro crie grupos de computadores com pelo menos um dispositivo ou consulta, na tela de rede. Você usará grupos e consultas para selecionar os dispositivos que estão incluídos nos relatórios.

Para executar um relatório de gestão de energia

1. Clique em **Ferramentas > Gerenciamento de energia > Gerenciamento de energia**.
2. Clique sobre uma das diretivas da pasta no modo de exibição de árvore e selecione a diretiva para a qual você quer executar o relatório.
3. Clique no botão **Relatórios** na barra de ferramentas e selecione **Economia** ou **Histórico.**
4. Clique em **Selecionar alvos**. Selecione os grupos ou consultas para os dispositivos que deseja incluir no relatório. Clique em **OK**.

   Os itens que você selecionar são listados, com um custo por kWh associado. O número total de máquinas nos grupos também é exibido.
5. Se você quiser calcular usando um custo por kWh diferente, alterar o número no campo **Custo por kWh.** Para remover um grupo ou consulta do relatório, clique no botão **Excluir**. Clique em **Atualizar relatório** para atualizar o gráfico após qualquer mudança.
6. Selecione um tipo de gráfico (potência ou economia financeira).
7. Selecione o símbolo de moeda que você deseja que o relatório apresente.
8. Sob o gráfico, selecione o período de tempo para o relatório (de 1 dia a 1 ano).

9. Para exportar uma cópia do relatório no formato .htm formato, clique em **Exportar** e especifique um local para salvar o arquivo.

NOTA: Para executar um relatório de histórico, você deve primeiro ter coletado dados históricos para dispositivos gerenciados (usando o botão **Dados históricos** da barra de ferramentas). Se você não tiver dados históricos, o relatório não vai criar um gráfico e não vai exportar um arquivo de relatório.

Usar dados históricos para relatórios de energia

Você pode coletar dados de uso de energia para dispositivos gerenciados se você deseja criar relatórios que representem o uso real do dispositivo durante um período de tempo. Os dados são armazenados no banco de dados e são usados quando você executa um relatório que inclua os dispositivos dos quais você coletou dados.

Use o botão **Dados históricos** da barra de ferramentas para iniciar e interromper a coleta de dados ou para excluir os dados do banco de dados.

Após coletar os dados de uso do cliente, você pode substituir os dados de uso do cliente padrão com dados históricos reais obtidos a partir dos seus dispositivos gerenciados.

Para substituir as pressuposições de uso do cliente pelos dados históricos

1. Na barra de ferramentas de Gerenciamento de energia, clique no botão **Personalizar** e selecione **Substituir pressuposições de uso do cliente com dados históricos**.
2. Selecione os grupos ou consultas dos quais você quer usar os dados históricos.
3. Selecione um período de tempo, ou seja, a última semana ou um período de tempo.
4. Clique em **Gerar tabela de uso padrão.**

Os novos dados são usados para gerar relatórios. Substitui os dados médios de uso usados como padrão para cálculo da economia de uso.

Tópicos relacionados

Instruções para usar estas opções de dados históricos são encontradas nos seguintes tópicos:

"Coletar informações de uso do cliente" na página 784

"Excluir os dados de utilização do cliente antigo" na página 785

Coletar informações de uso do cliente

Para coletar informações de uso do cliente

1. Clique em **Ferramentas > Gerenciamento de energia > Gerenciamento de energia**.
2. Clique no botão **Dados históricos** na barra de ferramentas e selecione uma ação (**Iniciar coleta informações de uso do cliente** ou **Interromper coleta de informações de uso do cliente**).

   Uma tarefa abre a janela **Tarefas agendadas**, identificada com a data e a hora.
3. Arraste dispositivos individuais, grupos ou consultas da tela de rede até a tarefa.
4. Para iniciar a tarefa agora, clique com o botão direito do mouse e selecione **Iniciar agora**.

5. Para agendar o início da tarefa para mais tarde, selecione a tarefa e clique em **Propriedades** na barra de ferramentas Tarefas agendadas. Clique em **Agendar tarefa > Iniciar mais tarde** e selecione as opções de agendamento.

Os dois painéis na ferramenta Tarefas agendadas exibe o progresso da tarefa, inclusive quais dispositivos não completaram a tarefa e por quê.

Excluir os dados de utilização do cliente antigo

Para excluir dados antigos de uso do cliente do banco de dados

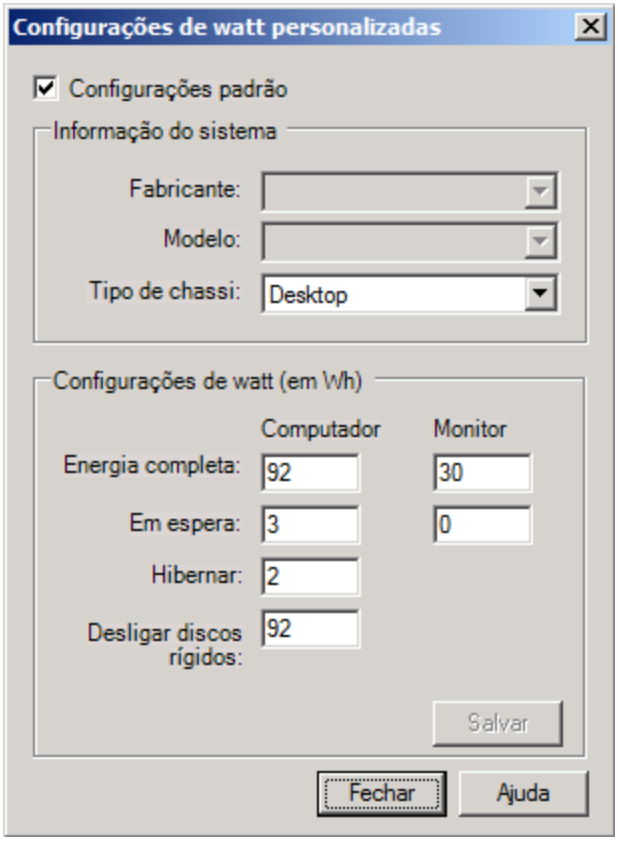
Após coletar os dados durante um período de tempo para elaboração de relatórios, você pode desejar excluí-los do banco de dados. Isto garante que os dados históricos são recentes.

1. Clique em **Ferramentas > Gerenciamento de energia > Gerenciamento de energia**.
2. Clique no botão **Dados históricos** na barra de ferramentas e selecione **Excluir dados antigos de uso do cliente**.
3. Especifique uma data e clique em **Excluir**.

As informações históricas de consumo e uso de energia anteriores a data especificada é excluída do banco de dados.

Personalizar configurações de potência elétrica

A ferramenta de Gerenciamento de energia inclui um utilitário que permite personalizar as configurações de consumo de voltagem para computadores similares a fim de oferecer um gerenciamento de energia mais preciso. As configurações que você selecionar e criar nesta caixa de diálogo são usadas nos cálculos de relatório.



Configurações padrão

As configurações padrão exibidas na caixa de diálogo **Personalizar configurações de consumo de voltagem** tem como base o tipo de computador que mencionado em um relatório.

Para um computador desktop, as configurações de potência elétrica padrão são baseadas nas configurações médias de um computador típico. Para laptops, as configurações padrão são menores porque os laptops normalmente usam menos energia.

Para mudar as configurações de potência elétrica padrão

1. Clique em **Ferramentas > Gerenciamento de energia > Gerenciamento de energia**.
2. Na barra de ferramentas, clique em **Personalizar** ( ) e selecione as **Configurações personalizadas de potência elétrica**.
3. Selecione o **Tipo de chassis** (desktop ou laptop).
4. Em **Computador**, altere as configurações de potência elétrica para especificar a potência elétrica usada pelo tipo de chassis selecionado, em diferentes formas de uso.
5. Nos campos do **Monitor**, altere as configurações de potência elétrica para especificar a potência elétrica usada pelo monitor quando em funcionamento ou em modo de espera.

Configurações personalizadas para modelos específicos

É possível utilizar configurações personalizadas pré-configuradas de energia para atender ao tipo de equipamento em uso. Muitas configurações para computadores desktop e laptops de fabricantes populares foram adicionadas para a sua conveniência.

Por exemplo, se você estiver monitorando a utilização de energia em um computador desktop Dell Inspiron 531s, selecione **Dell Inc.** na lista suspensa **Fabricante** e **Inspiron 531s** na lista suspensa **Modelo**. As configurações de consumo de voltagem do computador e de seu monitor foram adicionadas com base nos dados informados em um inventário LANDesk para um computador Inspiron 531s.

Adição de configurações de potência elétrica para modelos específicos de hardware

1. Clique em **Ferramentas > Gerenciamento de energia > Gerenciamento de energia**.
2. Na barra de ferramentas, clique em **Personalizar** ( ) e selecione as **Configurações personalizadas de potência elétrica**.
3. Desmarque a caixa de seleção **Configurações padrão**.
4. Selecione o **Fabricante** e **Modelo** para o tipo de dispositivo que você quer usar.
5. Clique em **Fechar** para salvar os dados para esse modelo.
6. Repita os passos 2-4 para cada modelo que você deseja incluir no cálculo de uso de energia.

As configurações de potência elétrica salvas são combinadas com os dispositivos gerenciados incluídos nos relatórios.

Configurações personalizadas para outros modelos

Quando a caixa de seleção **Configurações padrão é** selecionada, os campos das configurações de potência elétrica exibem o consumo médio de energia de um típico computador ou laptop. Após desmarcar a caixa de seleção **Configurações padrão**, use esses campos para digitar as configurações de uso de energia de marcas e modelos específicos de computadores que não fazem parte da lista de fabricantes e modelos.

Para adicionar configurações personalizadas de potência elétrica para outros modelos de hardware

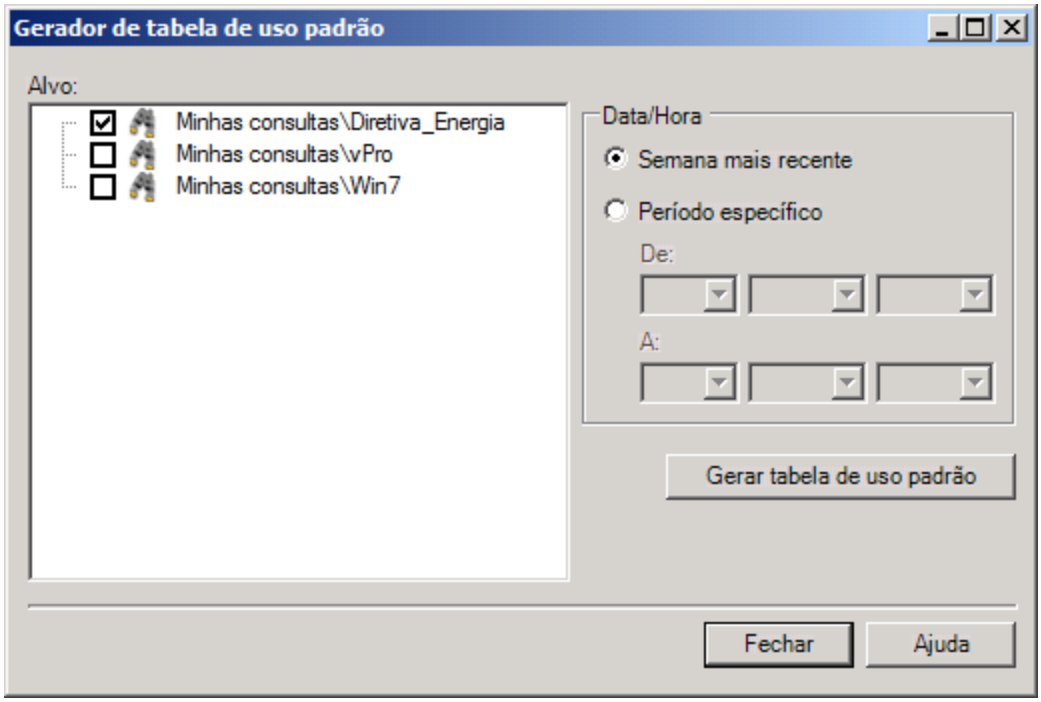
Se o tipo de equipamento que você deseja gerenciar não aparecer nas listas suspensas pré-configuradas **Informações de sistemas**, você pode digitar manualmente as informações necessárias. Para maior precisão, você vai precisar para reunir as informações de uso do fabricante.

1. Clique em **Ferramentas > Gerenciamento de energia > Gerenciamento de energia**.
2. Na barra de ferramentas, clique em **Personalizar** ( ) e selecione as **Configurações personalizadas de potência elétrica**.
3. Desmarque a caixa de seleção **Configurações padrão**.
4. Digite o nome do **Fabricante** e o nome/número do **Modelo** para o tipo de dispositivo que pretende usar.
5. Selecione o tipo de Chassis que corresponde ao dispositivo.
6. Adicione os dados de potência elétrica para o computador e para o monitor em diferentes estados de uso.
7. Clique em **Fechar** para salvar os dados para esse modelo.

Gerar um arquivo XML para cálculo de uso padrão

Relatórios de gerenciamento de energia usam médias de dados para diferentes tipos de computadores (desktop, notebook ou laptop). Ao gerar um relatório para um grupo de computadores, os computadores nesse grupo são combinados com a média de potência elétrica para os tipos de computadores correspondentes. Os dados baseiam-se, portanto, na média, mas não no uso específico.

Um arquivo XML contém os dados médios. Se você tiver recolhido dados históricos de seus dispositivos gerenciados, você pode gerar um novo arquivo XML que usa dados de seus dispositivos gerenciados em vez da média. Este arquivo XML substitui o arquivo padrão e reflete, assim, o uso de energia em sua empresa e fornece relatórios mais precisos da economia.



Para gerar um novo arquivo XML para cálculos de uso padrão

1. Clique em **Ferramentas > Gerenciamento de energia > Gerenciamento de energia**.
2. Na barra de ferramentas, clique no botão **Personalizar** ( ) e selecione **Substituir pressuposições de uso do cliente com dados históricos**.
3. Selecione os grupos de dispositivos ou consultas que você deseja usar para calcular os dados.
4. Selecione o intervalo de tempo do qual você quer calcular os novos dados. Você pode escolher a última semana ou especificar um período de tempo.
5. Clique em **Gerar tabela de uso padrão.**

Um novo arquivo XML é criado. Os dados deste arquivo serão usados nos cálculos do relatório de economia.

NOTA: Para gerar um novo arquivo de XML, você deve ter coletado dados históricos a partir de dispositivos gerenciados por, pelo menos, o período de tempo que você selecionar essa caixa de diálogo. Se não houver dados históricos suficientes, você não será capaz de gerar um novo arquivo XML.

Exibir o log de alertas de gerenciamento de energia

Como as diretivas de gestão de energia são executadas em dispositivos gerenciados, pode haver situações onde os dispositivos não respondem a ações de energia como esperado. Por exemplo, um processo executado em dispositivos podem continuar a funcionar mesmo quando um comando para alterar os estado de energia é enviada para o dispositivo.

O log de alerta lista os detalhes de tais conflitos. Você pode usar a informação deste log para gerenciar aplicativos em dispositivos, especificando quais aplicativos devem autorizados a continuar em execução ou desativados quando uma ação de energia estiver agendada.

Para exibir o log de alertas de gerenciamento de energia

1. Clique em **Ferramentas > Gerenciamento de energia > Gerenciamento de energia**.
2. Clique no nó do **Log de alerta** no modo de exibição de árvore.
3. Para encontrar alertas para um dispositivo específico, ou para um intervalo de dados, digite uma string de busca no campo **Localizar** e selecione uma coluna, ou selecione um intervalo de datas e clique no botão **Pesquisar**.

Após identificar os processos que geram conflitos, use as opções de **Gerenciamento de aplicativos** na barra de ferramentas para alterar a forma como a diretiva de energia é executada quando certos aplicativos são executados em um dispositivo. Para obter mais informações, consulte "Gerenciar aplicativos em conflito com as diretivas de energia" na página 779 .

Alertas

Visão geral de alertas e monitoramento

O Alerta e monitoramento do LANDesk Management Suite informa imediatamente dos eventos de hardware, software e aplicativos dos dispositivos que você gerencia. Quando ocorrem eventos que indicam a necessidade de ação ou um problema em potencial, os alertas iniciam as soluções ao fazer o log do evento, enviar uma mensagem de e-mail ou pager, executando um aplicativos ou desligando o dispositivo.

Os tipos normais de monitoramento a seguir estão disponíveis no Management Suite:

- Monitoramento (ping) da conectividade de rede de dispositivos
- Monitoramento básico de hardware e software de todos os dispositivos
- Monitoramento de desempenho de recursos de hardware selecionados
- Uso da tecnologia de monitoramento do fabricante em monitoramento dependente de hardware

O Management Suite oferece alerta integrado para esses diferentes tipos de monitoramento. Os alertas que você escolher aplicar à dispositivos específicos estão contidos nos conjuntos de regras que você distribuir.

Todos os alertas e monitoramento são dependentes do tipo de hardware, firmware e recursos relacionados para cada dispositivos. Algumas opções de monitoramento não são compatíveis em tipos de dispositivos diferentes. Em alguns casos a implementação de um padrão de hardware pode ser diferente entre fabricantes, portanto, o que funciona em um dispositivo pode não funcionar em outro.

Entendendo alertas, regras e conjuntos de regras

Um *alerta* é uma ID única que representa um evento. Você pode especificar uma *ação de alerta* a ser executada automaticamente quando ocorrer o evento, tais como um e-mail automático, aplicativos ou opções de energia.

Um alerta combinado com uma ação é mencionado neste produto como uma *regra de alerta*. Alguns alertas podem ser combinados com *regras de monitoramento de desempenho* específicas que especificam a condição que disparou um evento. Por exemplo, você pode definir uma regra de monitoramento para espaço disponível em disco em unidades de disco, para que, quando um disco esteja 90% cheio, seja gerado um alerta de aviso.

Ao definir os *Conjuntos de regras de alertas* você decide quais eventos exigem ação imediata ou precisam ser registrados para a sua atenção. Um conjunto de regras contém uma coleção de regras de alertas, cada uma com uma ação de alerta correspondente. Você pode distribuir conjuntos de regras de alertas para um ou mais dispositivos para monitorar os itens que são importantes para aquele tipo de dispositivo.

Conjuntos de regras e agentes de alertas

Para gerar alertas para um dispositivo gerenciado, o agente de alerta LANDesk deve ser distribuído para aquele dispositivo. Ao instalar o agente padrão no dispositivo, um agente de alerta padrão e um conjunto de regras de alerta são distribuídos para todos os dispositivos gerenciados. Aquele agente segue as regras definidas no conjunto de regras de alerta para aquele dispositivo.

Por padrão, cada dispositivo gerenciado possui um conjunto de regras de alerta padrão. Ao definir um conjunto de regras personalizado, você pode distribuí-lo para os dispositivos para monitorar itens específicos para aquele tipo de dispositivo. Você pode distribuir vários conjuntos de regras aos dispositivos, embora deva estar ciente de que podem ocorrer conflitos entre regras similares em diferentes conjuntos de regras.

NOTA: Ao instalar um console Win32 adicional a um dispositivo, nenhum agente é instalado nele. Mesmo que você possa gerenciar outros dispositivos a partir daquele console, ele não pode gerar alertas, seja um dispositivo núcleo ou gerenciado, a menos que você instale agentes de gerenciamento nele.

Entendendo o monitoramento de desempenho

Alguns eventos de alerta são baseados em regras específicas de monitoramento de desempenho. O *Monitoramento de desempenho* refere-se a um evento baseado nos contadores de desempenho definidos para dispositivos específicos. Os contadores podem ser definidos por componentes de hardware e sensores, desempenho de sistema operacional, componentes de aplicativos e níveis de uso.

Para adicionar a monitoramento de desempenho ao conjunto de regras para um dispositivo, selecione a regra de alerta "Monitoramento de desempenho" no conjunto de regras. Porém, os detalhes do que monitorar são definidos para cada dispositivo individualmente. Isto é feito no console de inventário e monitoramento em tempo real de cada dispositivo. Você pode selecionar componentes de hardware e software diferentes e definir contadores para itens a serem sondados e visualizar os dados de monitoramento em tempo real ou historicamente.

Monitoramento específico de hardware

O Management Suite inclui suporte para as seguintes tecnologias de monitoramento para hardwares de diferentes tecnologias:

- IPMI (Intelligent Platform Management Interface) 1.5 e 2.0
- Configuração do IPMI BMC (Baseboard Management Controller)
- Dell OMCI (OpenManage Client Instrumentation)
- Dell DRAC (Dell Remote Access Controller)
- Intel vPro technology, inclusive o Intel AMT (Active Management Technology)

Visão geral de Inventário e monitoramento em tempo real

O LANDesk Management Suite fornece atualizações em tempo real de dados de inventário e de status de monitoramento no console de Inventário e monitoramento em tempo real.

Este console está disponível somente para dispositivos que possuam o Agente LANDesk com as opções inventário e monitoramento em tempo real selecionadas.

Abertura do console

Você pode abrir o console de inventário e monitoramento em tempo real de duas formas:

- Clique com o botão direito em um dispositivo gerenciado no modo de exibição de rede e selecione **Inventário e monitoramento em tempo real**. Essa opção estará indisponível se a opção monitoramento não estiver selecionada no agente LANDesk do dispositivo.
- Abra o Dashboard funcionamento (clique em **Ferramentas > Relatórios/Monitoramento > Dashboard funcionamento**). Clique com o botão direito em um dispositivo e selecione **Exibir detalhes**. O console de Inventário e monitoramento em tempo real abre para todos os dispositivos, mas os dados em tempo real não são fornecidos se a opção de monitoramento não estiver selecionada no agente LANDesk do dispositivo.

Monitoramento de dispositivos para conectividade de rede

A monitoração de clientes permite monitorar periodicamente a conectividade de qualquer um dos dispositivos gerenciados.

As configurações de ping são específicas para o dispositivo selecionado. Quando um dispositivo para de responder a um ping (quando ele fica offline), é adicionado um alerta de notificação ao login no servidor núcleo. Se você quiser ser notificado com outra ação de alerta, como receber um e-mail quando um dispositivo fica offline, você pode configurar um alerta no conjunto de regras de alerta do núcleo.

Para monitorar conectividade para dispositivos gerenciados

1. Clique em **Configurar > Monitoramento de dispositivos**.
2. Clique em **Adicionar**. Selecione um ou mais dispositivos que você deseja monitorar e, em seguida, clique em **Adicionar**.
3. Especifique a configuração **Frequência de ping**, o número de tentativas e o limite de tempo.
4. Clique em **OK**.

Clique aqui para obter mais detalhes sobre a caixa de diálogo Configurar monitoramento de dispositivos.

Use essa caixa de diálogo para configurar as seguintes opções de monitoramento de dispositivos.

- **Monitorar estes dispositivos:** mostra os dispositivos que estão sendo monitorados.
- **Adicionar:** Abre a caixa de diálogo **Adicionar dispositivos monitorados** onde você poderá procurar e selecionar os dispositivos gerenciados que deseja monitorar.
- **Remover:** exclui o dispositivo selecionado da lista.
- **Freqüência de ping:** Controla quando e como a operação de ping ocorre. Essas configurações podem ser aplicadas aos dispositivos individualmente.
    - **Ping a cada:** agenda um ping periódico para o intervalo em minutos especificado.
    - **Agendar diariamente às:** agenda um ping diário em um horário específico.
    - **Novas tentativas:** especifica o número de novas tentativas de ping.
    - **Tempo limite:** especifica o número de segundos até as novas tentativas de ping atingirem o tempo limite.

Configuração de alertas de monitoramento de dispositivos

Se você quiser que o monitoramento de dispositivo o notifique quando dispositivos gerenciados ficarem online ou offline, você precisa primeiro configurar um conjunto de regras de alerta que tenha ações adicionais (como receber um e-mail quando o alerta for enviado).

Para configurar os alertas de monitoramento de dispositivos

1. Clique em **Ferramentas > Configuração > Alerta**.
2. Na árvore **Alertas**, expanda o item **Conjuntos de regras de alerta**.
3. Clique com o botão direito em **Conjuntos de regras de alerta do núcleo** e clique em **Editar**.
4. No painel à esquerda **Conjunto de regras de alerta** da janela **Conjunto de regras**, clique em **Alertas**.
5. No painel **Alertas**, sob a pasta **Padrão**, clique em **Monitor de dispositivos**.

6. No painel direito, clique em **Regras > Adicionar**.
7. Arraste o alerta **Conectivity do sistema do monitor de dispositivos** para os **Alertas** na parte inferior da página.
8. No painel **Conjunto de regras de alerta** da esquerda na janela **Conjunto de regras**, clique em **Ações** e arraste qualquer ação adicional que quiser para o compartimento **Ações**. Como padrão a configuração do identificador do log de alerta do núcleo é a ação. Você pode escolher enviar um e-mail ou uma interceptação de SNMP, ou abra um arquivo executável no núcleo quando o alerta for recebido. (Você precisa definir cada ação, tal como especificar para onde enviar alertas por e-mail.)
9. No painel à esquerda **Conjunto de regras de alerta** da janela **Conjunto de regras** clique em **Hora** e arraste **Sempre** ao compartimento **Hora**.
10. Clique no botão **OK** próximo aos compartimentos.
11. No painel **Ações** à direita, clique em **Publicar**.
12. No painel **Conjunto de regras de alerta** à esquerda, clique em **Resumo das regras** e clique duas vezes na regra que você criou.
13. Na caixa de diálogo exibida, marque a caixa **Funcionamento** se desejar que o status de funcionamento de um dispositivo no console mude quando estiver online/offline e clique em **OK**.
14. Clique em **Publicar** para publicar as mudanças que você fez e feche a janela **Conjunto de regras.**

NOTA: Quando são definidas, as configurações de alerta aplicam-se a todos os dispositivos que estão sendo monitorados.

Desativação do serviço ModemView

ModemView é o serviço/driver que monitora as chamadas de modem (recebidas e enviadas) e gera um alerta ao detectar uma chamada. Esse serviço utiliza aproximadamente 10 Mb de memória, pois usa o MFC. Recomenda-se que esse serviço seja desativado, especialmente se não houver um modem no dispositivo.

Para desativar o serviço ModemView

1. No dispositivo (diretamente ou via controle remoto) clique em **Iniciar > Painel de controle > Ferramentas administrativas > Serviços**.
2. Clique duas vezes em **LANDesk Message Handler Service** (Serviço de manipulação de mensagem LANDesk).
3. Em **Tipo de inicialização**, selecione **Manual** e clique em **OK**.

Você também pode clicar na opção **Parar** em **Status de serviço**.

Noções básicas sobre alertas

Para gerar alertas para um dispositivo gerenciado, o agente de alerta do Management Suite deve ser distribuído para aquele dispositivo. Ao instalar o agente padrão no dispositivo, um agente de alerta padrão e um conjunto de regras de alerta são distribuídos para todos os dispositivos gerenciados. Aquele agente segue as regras definidas no conjunto de regras de alerta para aquele dispositivo.

Ao definir um conjunto de regras personalizado, você pode distribuí-lo para os dispositivos para monitorar itens específicos para aquele tipo de dispositivo. Você pode distribuir vários conjuntos de regras aos dispositivos, embora deva estar ciente de que podem ocorrer conflitos entre regras similares em diferentes conjuntos de regras.

Eventos que podem gerar alertas

Este produto tem uma lista extensa de eventos que podem gerar alertas. Alguns eventos são problemas que necessitam de atenção imediata, tais como falha de um componente ou desligamento do sistema. Outros eventos são alterações de configurações que fornecem informações úteis a um administrador de sistema, tais como alterações que afetam o desempenho e instabilidade de um dispositivo ou causam problemas com uma instalação padrão.

Os exemplos de tipos de eventos que podem ser monitorados incluem:

- **Mudanças de hardware:** Um componente como, por exemplo, processador, memória, unidade de disco ou placa de rede adicionada ou removida.
- **Aplicativos adicionados ou removidos:** Um usuário instalou ou desinstalou um aplicativo em um dispositivo. Isto pode ser útil no acompanhamento de licenças e da produtividade de funcionários. Os aplicativos registrados em Adicionar ou Remover programas do Windows são monitorados e o nome do aplicativo ali usado é o nome que aparece na notificação de alerta.
- **Evento de serviço:** Um serviço foi iniciado ou parado no dispositivo.
- **Desempenho:** Um limite de desempenho foi ultrapassado, como por exemplo, a capacidade de unidade de disco, memória disponível etc.
- **Evento IPMI:** Ocorreu um evento detectável nos dispositivos IPMI, que inclui mudanças em controladores, sensores, logs etc.
- **Uso do modem:** O modem do sistema foi utilizado ou foi adicionado ou removido um modem.
- **Segurança física:** Ocorreu uma intrusão no chassi, ciclagem de alimentação ou outra mudança física.
- **Instalação do pacote**: Foi instalado um pacote no computador alvo.
- **Atividade do controle remoto:** Ocorreu uma atividade de sessão de controle remoto, o que inclui iniciar, parar ou falhas.

Para exibir um registro dos alertas de mudanças na configuração, consulte o log de alertas no console de monitoramento e inventário em tempo-real do dispositivo.

Os alertas só podem ser gerados quando os dispositivos estão equipados com o hardware apropriado. Por exemplo, os alertas gerados por leituras de sensor só são aplicáveis a dispositivos equipados com os sensores corretos.

A monitoração de hardware também depende da configuração correta do hardware. Por exemplo, se um disco rígido com capacidades de monitoração S.M.A.R.T. for instalado em um dispositivo mas a detecção S.M.A.R.T. não for habilitada nas configurações do BIOS do dispositivo, ou se o BIOS do dispositivo não suportar unidades S.M.A.R.T., os alertas não serão gerados a partir da monitoração da unidade S.M.A.R.T.

Níveis de severidade para os eventos

Problemas ou eventos podem ser associados a alguns ou a todos os níveis de gravidade mostrados. Em algumas partes da interface do produto, esses estados são observados associados a um valor numérico e ícone. Os valores numéricos estão entre parêntesis.

- **Informativo (1)**: Suporta mudanças de configuração ou eventos que os fabricantes incluem em seus sistemas. Esse nível de gravidade não afeta o funcionamento do dispositivo.
- **OK (2)**: Indica que o status é um nível aceitável.

- **Aviso (3)**: Fornece algum tipo de advertência antecipada de um problema antes deste atingir um ponto crítico.
- **Crítico (4)**: Indica que o problema precisa de atenção imediata.
- **Desconhecido:** Não é possível determinar o status de alerta ou o agente de monitoração não foi instalado no dispositivo.

Dependendo da natureza de um evento, alguns níveis de severidade não se aplicam e não são incluídos. Por exemplo, no caso do Evento de detecção de intrusão, o gabinete do dispositivo está aberto ou fechado. Se estiver aberta, uma ação de alerta pode ser disparada, mas somente com a severidade de Aviso. Outros eventos, tais como Espaço em disco e Memória virtual, incluem três níveis de severidade (OK, Aviso e Crítico) porque os diferentes estados podem indicar diferentes níveis relativos ao administrador.

Você pode escolher o nível de severidade ou limite que dispara alguns alertas. Por exemplo, você pode selecionar uma ação para um status de Aviso e uma ação diferente para um status Crítico para um alerta. O status desconhecido não pode ser selecionado como um disparador de alerta, ele só indica que o status não pode ser determinado.

Ações de alerta para notificações

Este produto pode notificá-lo ao ocorrer eventos monitorados através de uma das seguintes ações:

- Adicionar informações ao log
- Enviar um aviso por e-mail ou enviar uma mensagem para um pager
- Executar um programa no núcleo ou em um dispositivo individual
- Enviar uma interceptação SNMP para um console de gerenciamento de SNMP na rede
- Reinicializar ou desligar um dispositivo

Ações de alerta são configuradas quando os conjuntos de regras de alerta são definidos.

Controle de alerta de 'inundação'

Certos alertas designados a grupos de dispositivos podem gerar simultaneamente um grande número de respostas. Por exemplo, você pode incluir a regra de alerta para alterações da configuração do computador e associá-la a uma ação de e-mail. Se um patch de distribuição de software for aplicado a muitos dispositivos com essa configuração de alerta, esta ação gera um número de e-mails do servidor núcleo igual ao número de dispositivos aos quais o patch foi aplicado, potencialmente inundando seu servidor de e-mail com uma "avalanche" de notificações de alerta.

Este recurso de controle de alerta de inundação do produto limita automaticamente o número de vezes que uma ação de alerta ocorre para um alerta. Se um alerta dispara uma ação 5 vezes em 5 minutos, a ação de alerta é descontinuada mas os alertas ainda são gravados no arquivo de log núcleo. O administrador é notificado da inundação de alertas com um e-mail automático. Quando o alerta cessa e não ocorre novamente por uma hora, o controle de inundação de alerta é redefinido para aquele alerta. As ações de alerta serão disparadas novamente se aquele alerta ocorrer novamente.

Distribuição do conjunto de regras de alerta

Este produto inclui conjuntos de regras de alerta pré-definidos que podem ser distribuídos para dispositivos gerenciados. Observe que cada dispositivo gerenciado deve ter um agente de gerenciamento instalado antes de poder distribuir um conjunto de regras de alerta e antes de enviar os alertas ao servidor núcleo.

Conjunto de regras padrão

Quando o agente de monitoramento é instalado em um dispositivo gerenciado, o conjunto de regras **Padrão do LDMS** é instalado para fornecer feedback de status do funcionamento para o dashboard funcionamento e ao console. O conjunto padrão de regras contém alertas do tipo:

- disco adicionado ou removido
- espaço na unidade
- uso da memória
- temperatura, ventiladores e voltagens
- atividades do controle remoto
- Monitoramento do desempenho
- eventos de IPMI (em hardwares aplicáveis)
- Alertas do analisador de inventário
- Ações do gerenciador de controle de conexão
- Status do antivírus do LANDesk
- Status do controle de acesso à rede
- Utilitário do banco de dados cliente
- Alertas de Segurança e Gerenciador de patch

Você pode modificar o conjunto de regras de alerta LDMS padrão para incluir os alertas que deseja monitorar.

Personalizar conjuntos de regras de alerta

Além do conjunto padrão de regras, você pode configurar e distribuir conjuntos personalizados de regras. Você pode incluir ações de alerta personalizadas para responder a uma combinação de eventos. Por exemplo, você pode desejar definir um conjunto de ações para evento em dispositivos desktop gerenciados (tais como envio de e-mail à equipe de suporte de hardware) e um diferente conjunto de ações para os servidores gerenciados (tal como o envio de uma mensagem de pager ao admin).

Processo para a distribuição do conjunto de regras

O processo geral para distribuição de conjuntos de regras de alertas para dispositivos gerenciados é feito da seguinte maneira:

1. Criar ou editar um conjunto de regras.
2. Crie uma tarefa para agendar a distribuição do conjunto de regras
3. Selecione os dispositivos para os quais você distribuirá o conjunto de regras e execute a tarefa agendada.
4. Se um conjunto de regras inclui alertas do monitor de desempenho, abra o console de inventário e monitoramento em tempo real para cada dispositivo com esse conjunto de regras e defina contadores de monitoramento de desempenho para os dispositivos

Tópicos relacionados

"Configuração de conjunto de regras de alerta" na página 799

"Distribuir um conjunto de regras de alertas" na página 797

"Sobre o desempenho do monitoramento" na página 812

"Usar configurações de agente" na página 101

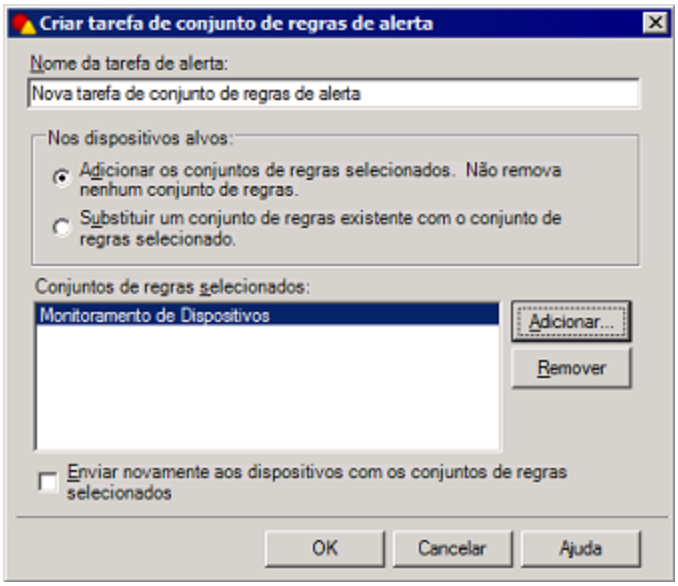
Distribuir um conjunto de regras de alertas

Para instalar um conjunto de regras de alerta em um ou mais dispositivos, você pode agendar uma tarefa de distribuição para o conjunto de regras.

A fim de distribuir um conjunto de regras a um dispositivo gerenciado, é necessário primeiro instalar um agente de gerenciamento naquele dispositivo. Ao distribuir o agente de gerenciamento padrão, o conjunto de regras padrão é instalado no dispositivo, por padrão mas, você pode selecionar este ou qualquer outro conjunto de regras disponíveis a ser instalado no dispositivo com o agente de gerenciamento. Após a configuração do agente ser completada, você pode atualizar o conjunto de regras padrão ou distribuir novos conjuntos de regras agendando uma tarefa de alerta.

Para distribuir um conjunto de regras de alerta

1. Clique em **Ferramentas > Configuração > Alerta**.
2. Na lista **Conjuntos de regras de alerta**, clique no conjunto de regras que desejar distribuir.
3. Na barra de ferramentas, clique no ícone **Criar uma tarefa** e selecione **Distribuir conjunto de regras**.


Criar tarefa de conjunto de regras de alerta
Nome da tarefa de alerta:
Nova tarefa de conjunto de regras de alerta
Nos dispositivos alvos:
Adicionar os conjuntos de regras selecionados. Não remova nenhum conjunto de regras.
Substituir um conjunto de regras existente com o conjunto de regras selecionado.
Conjuntos de regras selecionados:
Monitoramento de Dispositivos
Adicionar...
Remover
Enviar novamente aos dispositivos com os conjuntos de regras selecionados
OK
Cancelar
Ajuda

4. Digite um nome de tarefa para a tarefa de alerta.
5. Para adicionar um conjunto de regras à dispositivos e manter os conjuntos de regras nos dispositivos, clique em **Adicionar conjuntos de regras selecionadas**.

   Para adicionar um conjunto de regras à dispositivos e remover os conjuntos de regras nos dispositivos, clique em **Substituir todos os conjuntos de regras**.

   Se você distribuiu anteriormente o conjunto de regras e deseja atualizá-lo nos mesmos dispositivos, marque a caixa de seleção **Reenviar aos dispositivos com o conjunto de regras selecionados**.
6. Para distribuir os outros conjuntos de regra na mesma tarefa, clique no botão **Adicionar** e selecione o conjunto de regras.

7. Clique em **OK**.

   Uma nova tarefa é criada na ferramenta **Tarefas agendadas**.

8. Arrastas dispositivos do modo de exibição de rede para a nova tarefa de alerta.
9. Clique com o botão direito do mouse na tarefa e selecione **Propriedades**. Certifique-se de ter os dispositivos alvo corretos e selecione as opções para agendá-los e clique em **Salvar**.

Notas

- Você pode distribuir os conjuntos de regra aos dispositivos como parte de uma configuração de agente. Ao definir uma configuração de agente, você pode selecionar o conjunto de regras que deseja distribuir.
- Se o conjunto de regras que você distribuir incluir uma regra de monitoramento de desempenho, os detalhes do que é monitorado são definidos individualmente em cada dispositivo. Isto é feito no console de inventário e monitoramento em tempo real de cada dispositivo. Você pode selecionar componentes de hardware e software diferentes e definir contadores para itens a serem sondados e visualizar os dados de monitoramento em tempo real ou historicamente.

Tópicos relacionados

"Crie uma configuração de agente" na página 102

"Sobre o desempenho do monitoramento" na página 812

Visualização dos conjuntos de regras de alerta de um dispositivo

Para visualizar um conjunto de regras de alerta atribuídos a um dispositivo gerenciado, abra a visualização completa do inventário para o dispositivo. Isso exibirá o nome do conjunto de regras e a data em que o dispositivo foi instalado ou atualizado pela última vez.

Para visualizar o conjunto de regras de alertas em um dispositivo

1. Em **Todos os dispositivos**, clique com o botão direito no dispositivo e selecione **Inventário**.
2. Na visualização em árvore, expanda **LANDesk Management** e clique em **Conjunto de regras de alertas instalado**.
3. Se houver mais de um conjunto de regras, selecione um deles na visualização em árvore para exibir seus detalhes.

NOTA: Você pode criar uma consulta que retorne todos os dispositivos que possuam um conjunto de regras de alerta em particular instalados. Na lista de componentes da consulta, siga o mesmo caminho descrito na lista de inventário acima.

Remover todos os conjuntos de regras de um dispositivo

Você pode remover todos os conjuntos de regras de um ou mais dispositivos sem distribuir novos conjuntos de regras.

Você pode remover todos os conjuntos de regras se você tem um ou mais conjuntos de regras em efeito em um dispositivo e quer substituí-lo por um novo conjunto de regras. Após efetivar vários conjuntos de regras em um dispositivos, resultados imprevisíveis podem ocorrer devido a conflitos de regras similares e resultados não intencionais podem ocorrer.

Para remover todos os conjuntos de regras existentes

1. Clique em **Ferramentas > Configuração > Alerta**.
2. Na barra de ferramentas, clique no ícone **Criar uma tarefa** e selecione **Remover conjuntos de regras**.
3. Clique em **OK**.

Migração de alertas de versões anteriores

As versões anteriores do LANDesk Management Suite incluem a funcionalidade de alerta com o recurso Alert Management System (AMS). Começando com a versão 8.8, o alerta é baseado em um novo conjunto de identificadores de alerta, até mesmo alguns alertas baseados em alertas AMS. Seu conjunto de regras de alerta para dispositivos gerenciados precisará ser criado usando o novo recurso de alerta.

Para ajudá-lo a migrar alertas das versões anteriores a 8.8, este produto inclui um utilitário que extrai as informações sobre seus alertas AMS e grava os dados em um arquivo de texto, que você pode consultar conforme cria novos conjuntos de regras.

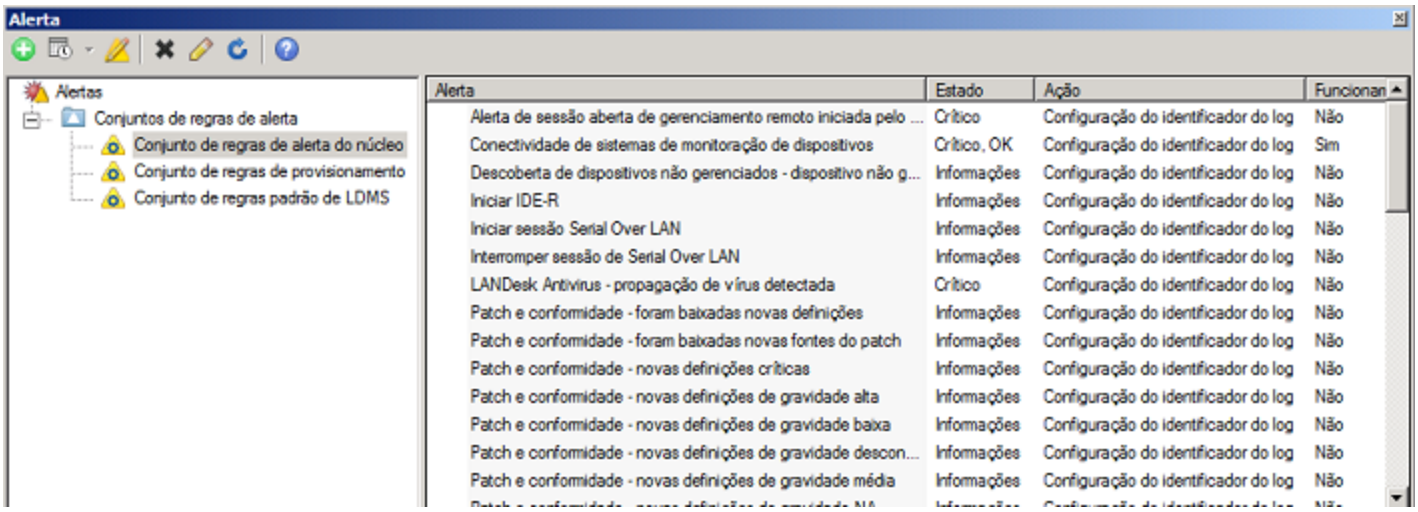
Para usar o utilitário de alerta de migração

1. No diretório \utilities no compartilhamento LDMAIN, execute alertexp.exe.
   Para exibir as informações de ajuda sobre o uso do utilitário, digite `alertexp.exe /?` na linha de comando. Você pode especificar opcionalmente o caminho para o arquivo iaobind.dat e um caminho e um nome de arquivo para o arquivo de saída.
2. Abra o arquivo iaobind.txt para ver um resumo dos alertas AMS existentes.

Você pode usar as informações sobre os alertas existentes para criar novos conjuntos de regras de alertas. O arquivo de texto lista o nome de cada alerta com a ação associada e a severidade, juntamente com o aplicativo que dispara o alerta e os parâmetros associados a ele.

Configuração de conjunto de regras de alerta

A página **Conjunto de regras de alertas** mostra todos os conjuntos de regras de alerta que podem ser distribuídos aos dispositivos gerenciados. Existem quatro conjuntos de regras que aparecem por padrão e você pode criar conjuntos de regras personalizados para aplicar a tipos específicos de monitoramento para os diferentes tipos de dispositivos.



Os quatro conjuntos de regras de alerta são mostrados na página **Conjuntos de regras de alerta**:

- **Conjunto de regras de alerta núcleo**: Este conjunto de regras garante que os alertas originados no servidor núcleo sejam identificados. Este conjunto de regras é instalado no servidor núcleo, mas não pode ser instalado em outros dispositivos e, você somente pode ter um conjunto de regras de alerta núcleo. Você pode editar o conjunto de regras, mas não pode excluí-lo do servidor núcleo. Este conjunto de regras contém um grupo pré-definido de tipos de alerta, inclusive Monitor de dispositivos, alertas Intel vPro e de Sessão Serial Over LAN.
- **Conjunto de regras padrão LDMS**: Este conjunto de regras é distribuído por padrão a todos os dispositivos gerenciados pelo LANDesk Management Suite. Ele inclui alertas para recursos de segurança incluídos no Management Suite, tais como, Inventário e monitoramento em tempo real, controle de acesso de rede, analisador de inventário e alertas do Gerenciador de segurança e patch.
- **Conjunto de regras de provisionamento**: Este conjunto de regras contém os alertas relacionados as tarefas de provisionamento, tais como início e fim da tarefa, seção completa e ambiente errado pré-reinicialização SO. Ao provisionar um dispositivo, este conjunto de regras é usado para enviar alertas relacionados ao progresso da tarefa de provisionamento. O conjunto de regras está incluso no agente de provisionamento e não precisa ser distribuído manualmente. Você pode editar este conjunto de regras para alterar a ação associada aos alertas de provisionamento (por exemplo, ser notificada por e-mail quando uma tarefa de provisionamento for concluída).

Além desses conjuntos de regras, você pode criar conjuntos personalizados e aplicá-los à grupos de dispositivos gerenciados. Você pode distribuir conjuntos de regras agendando uma tarefa de distribuição ou pode incluir conjuntos de regras ao distribuir agentes para os dispositivos usando a configuração de agente. Como os conjuntos de regra padrão estão disponíveis para serem distribuídos com agentes, você pode escolher não distribuí-los quando definir a configuração do agente.

Conflitos entre conjunto de regras

Ao criar um conjunto de regras personalizado para um dispositivo observe que, se um conjunto padrão já tiver sido distribuído para o dispositivo, poderá haver sobreposição ou conflito de regras de alerta. Se você distribuir o conjunto de regras quando configurar o dispositivo gerenciado e, em seguida, distribuir um conjunto de regras personalizado, ambos os conjuntos serão executados no dispositivo.

Por exemplo, se ambos os conjuntos de regras alertarem com o mesmo tipo de alerta, mas executarem ações diferentes, pode ocorrer ações de alerta duplicadas ou imprevisíveis.

Ação de log padrão

Cada vez que você cria uma regra de alerta, uma regra é automaticamente criada com uma ação "Configuração do identificador do log". Isso acontece para que cada alerta efetue log no servidor núcleo.

Esta regra padrão deve estar sempre no conjunto de regras: você não pode excluir a menos que exclua todas as regras para aquele alerta em particular. Em outras palavras, se houver três regras para um alerta, você não pode excluir a regra padrão a menos que exclua todas as três regras, porém, você pode excluir qualquer uma das outras duas.

Processo para configuração de um conjunto de alertas

Os conjuntos de alerta contém uma coleção de alertas, ações e filtros de tempo associados. Ao configurar um conjunto de regras, você definirá as várias tarefas e filtros de tempo que podem ser reutilizados. O procedimento geral para a configuração de um conjunto de regras inclui as seguintes etapas:

1. Criar um conjunto de regras
2. Adicionar novas regras de alerta a um conjunto de regras
3. Definir as ações de alerta a serem usadas nas regras
4. Definir os filtros de tempo a serem usado nas regras de alerta
5. Editar as regras de alerta em um conjunto de regras
6. Incluir conjuntos de regras com outros conjuntos de regras
7. Publicar um conjunto de regras

Clique aqui para um exemplo de como configurar um conjunto de regras.

Exemplo: Configuração de um conjunto de regras de alerta para problemas de espaço em disco

Os procedimentos a seguir demonstram um simples exemplo do primeiro passo em configurar um conjunto de regras de alerta personalizado. Neste exemplo, uma única regra de alerta é adicionada ao conjunto de regras.

1. No console do servidor núcleo, clique em **Configuração > Alertas**.
2. Na barra de ferramentas, clique em **Novo**. Digite o nome do conjunto de regras e uma descrição (tal como "Espaço em disco 90% cheio") e clique em **OK**.
3. Na lista **Conjunto de regras de alerta**, clique no nome do novo conjunto de regras de alerta e clique em **Editar** na barra de ferramentas.
4. Na janela **Configuração do conjunto de regras**, clique em **Alertas** na coluna da esquerda.
   Uma visualização em árvore dos alertas é exibida, com uma grade contendo os alertas e suas descrições. Você pode clicar em **Todos os alertas** para visualizar todos os alertas disponíveis ou clicar em uma categoria na árvore para visualizar um grupo específico de alertas. Dependendo da resolução da sua tela, você pode redimensionar as colunas para ler os itens da lista.
5. Na tela da árvore, no grupo **Monitor**, clique no alerta **Espaço em disco**.
6. Na grade, selecione **Uso padrão de disco** e clique em **Editar** na coluna da direita.
7. Na caixa de diálogo **Monitoramento de espaço em disco**, você pode definir a freqüência do **Intervalo de sondagem** para mudar a freqüência com que o uso de espaço em disco será monitorado. Para alterar os limites nos quais os alertas são disparados, clique em **Espaço em disco** e defina as porcentagens para os alertas de aviso e crítico. (As porcentagens são do total ocupado de espaço disponível em disco.) Clique em **OK** para salvar as configurações.
8. Na coluna direita da página **Alertas**, clique em **Regras > Adicionar**.
   Três "compartimentos" são exibidos na parte inferior da página. Use os compartimentos para combinar alertas, ações e itens de tempo para criar uma regra de alerta.
9. Arraste o alerta **Uso padrão de disco** para o poço **Alertas**.
10. Na coluna esquerda, clique em **Ações**. Clique na pasta **Padrão Nova**. Arraste **Registrar alerta em log de evento local NT** para o compartimento **Ações**.
    Para cada regra de alerta que você criar, uma ação **Configuração do identificador do log** já está incluído no compartimento **Ações**. Se desejar adicionar outras ações, tais como envio de e-mail, você precisará definir uma ação e arrastá-la para o poço Ações.
11. Na coluna esquerda, clique em **Tempo**. Na lista Tempo, arraste **Sempre** para o poço **Tempo**.

12. Clique em **OK** próximo aos compartimentos para salvar a regra, em seguida clique em **OK** novamente na mensagem de sucesso.
    Você criou uma regra de alerta que faz parte do conjunto de regras. Para salvar as mudanças, é necessário publicar o conjunto de regras.
13. Na coluna da direita, clique no botão **Publicar**.
    Você pode voltar para a página **Resumo de regras** para visualizar a regra e, se desejar, editá-la.
14. Na coluna direita, clique em **Resumo de regras**.
    Observe que existem duas regras relacionadas. Uma é para a regra que você criou (com a ação **Registrar alerta em log de evento local NT**) e a outra é uma regra padrão que envia notificações de alerta para o servidor núcleo (com a **ação Configuração do identificador de log**). Esta é criada automaticamente para toda regra que você definir, deste modo, todos os alertas são registrados no servidor núcleo. Você não pode excluir esta regra a menos que exclua todas as regras para um alerta.
15. Selecione a regra **Uso padrão de disco** com **Registrar alerta em log de evento local NT** como a ação e clique em **Regras > Editar** na coluna direita. Use esta caixa de diálogo para alterar as configurações para a regra.
16. Para alterar a ação associada à regra, selecione um item diferente na lista suspensa **Ação**.
17. Para alterar o tempo durante o qual a regra de alerta está ativa, selecione um item diferente na lista suspensa **Tempo**.
18. Para mudar os níveis de severidade para as notificações de alerta, clique nos ícones **Estado**. Um ícone esmaecido não será usado, por isso, para receber os alertas somente para alertas de estado crítico, clique no ícone Aviso (Estado 2), um triângulo amarelo, para desativá-lo.
19. Selecione a caixa de seleção **Funcionamento** para incluir o uso de espaço em disco como um alerta que contribua para o status de funcionamento do dispositivo.
20. Clique em **OK**. Você pode ver as mudanças que fez na lista **Resumo de regras**.
    Para salvar as mudanças neste conjunto de regras você precisa publicá-las novamente. Em seguida, ele será salvo e estará disponível para distribuição na sua lista de conjunto de regras.
21. Na coluna da direita, clique em **Publicar**.

Quado você volta para o console de gerenciamento, o novo conjunto de regras criado aparece em **Conjunto de regras de alerta**.

Criar um conjunto de regras de alertas

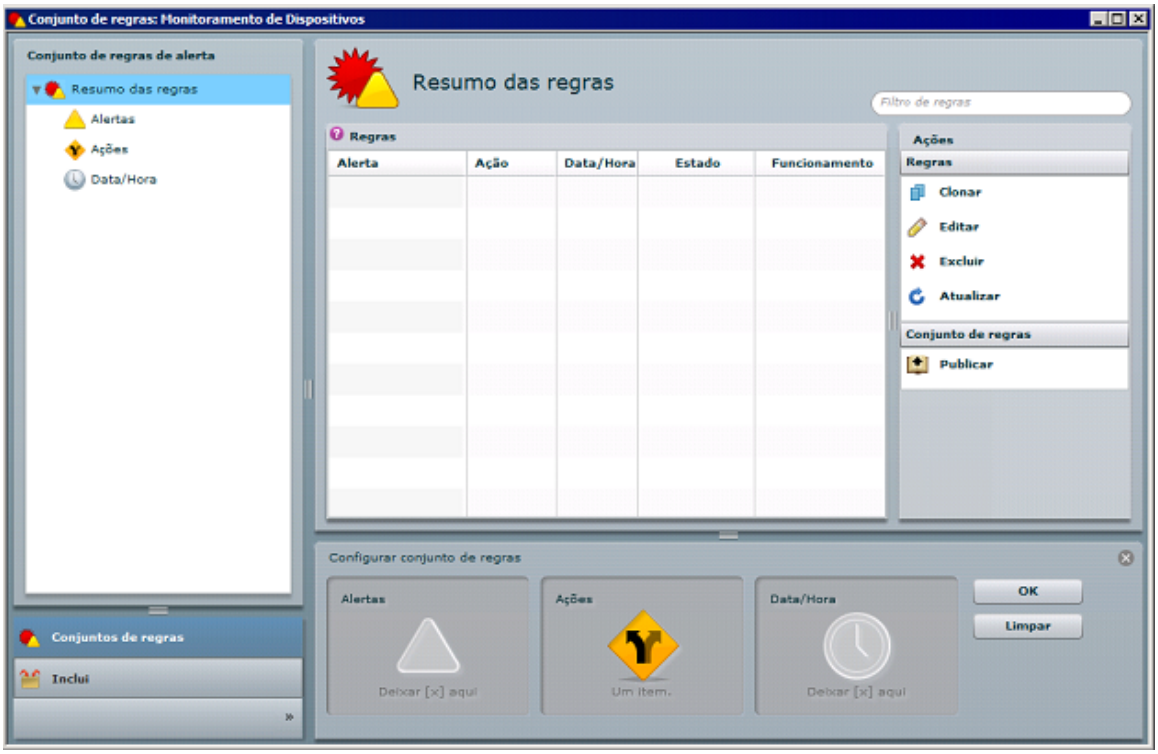
1. Clique em **Ferramentas > Configuração > Alerta**.
2. Clique no botão **Novo conjunto de regras de alerta** na barra de ferramentas. Digite um nome no campo **Nome**, digite uma descrição de alerta no campo **Descrição** e clique em **OK**.
3. Para mudar o nome ou a descrição do conjunto de regras, selecione-o na lista **Conjunto de regras de alerta** e clique no botão na barra de ferramentas **Editar um conjunto de regras de alerta**.
4. Para fazer uma cópia do conjunto de regras no qual você deseja fazer pequenas alterações, clique com o botão direito o conjunto de regras na lista e selecione **Copiar**. Digite um novo nome e descrição e clique em **OK**.

Após criar um conjunto de regras, edite o conjunto de regras para adicionar alertas e ações associadas.

Editar um conjunto de regras de alerta

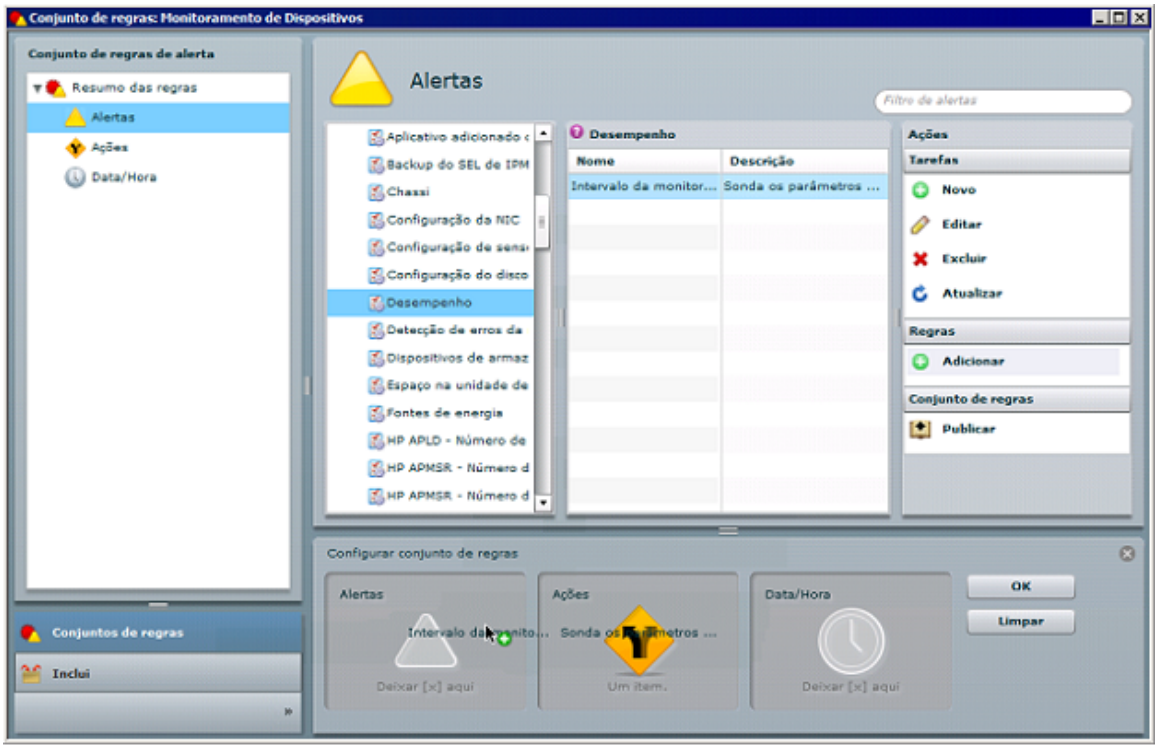
1. Na lista **Conjunto de regras de alerta**, selecione o conjunto de regras e clique em **Editar** na barra de ferramentas.

   A página **Resumo de regras** relaciona cada alerta no conjunto de regras com suas ações e hora associados. Cada combinação de um alerta, ação e tempo é listado como um item separado no resumo das regras.



2. Clique em **Alertas** na coluna da esquerda para adicionar uma regra de alerta ao conjunto de regras.

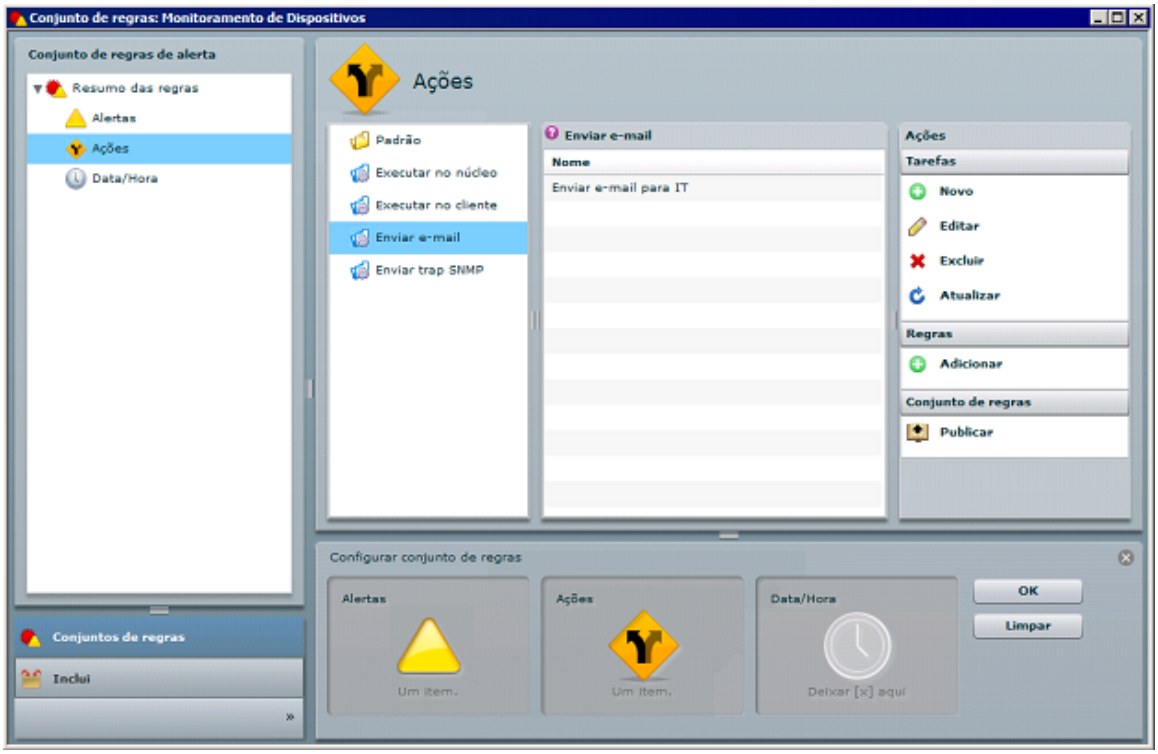
3. Na coluna direita, clique em **Regras > Adicionar**. Três "poços" são exibidos na parte inferior da página para associar os alertas, as ações e as regras de tempo. Localize um alerta na lista e arrate-o para o compartimento **Alertas** na parte inferior da página.



Os alertas são relacionados em dois grupos, **Padrão** e **Monitor**. Clique em um item em um daqueles grupos para visualizar um grupo de alertas associados. Se clicar na pasta **Todos os alertas**, todos os alertas são listados em ordem alfabética.

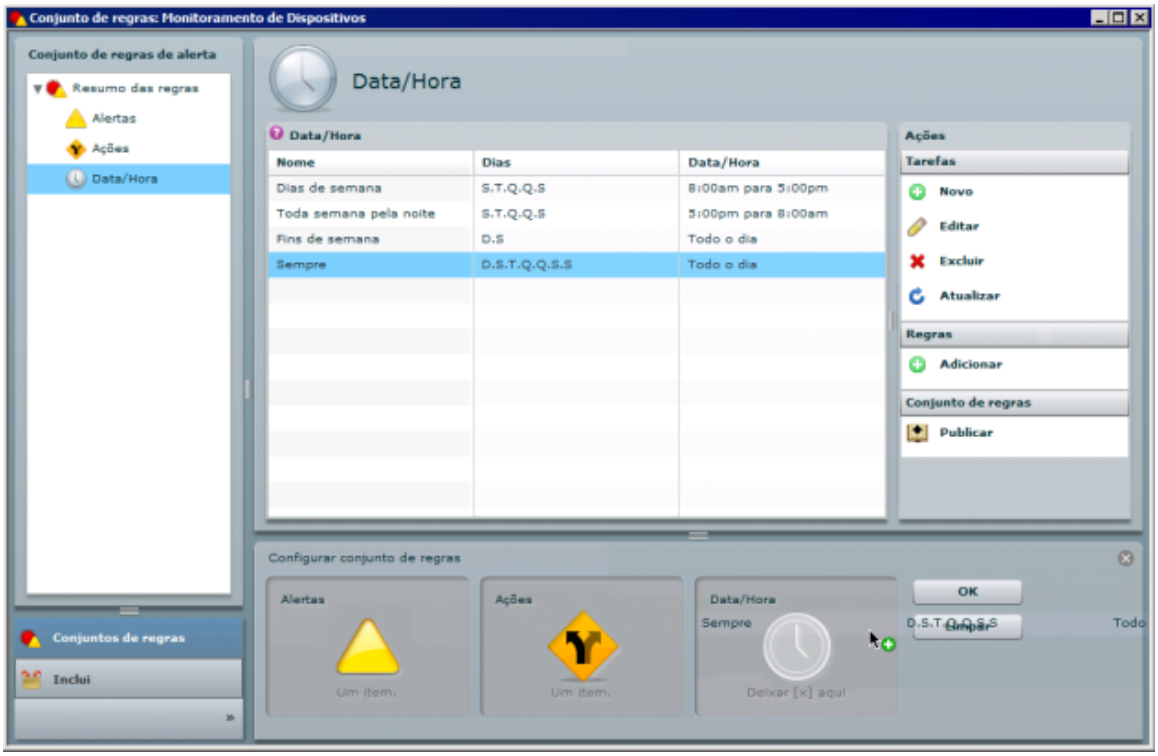
4. Para localizar um alerta em particular, digite uma string de pesquisa na caixa de texto **Filtro de alertas** na parte superior direita da página. Todos os alertas contendo a string que você digitar serão exibidos na lista.

5. Clique em **Ações** para associar uma ação de alerta com o alerta adicionado. Por padrão, cada alerta possui uma ação **Configuração de identificador de log** associado, que faz a conexão do alerta no servidor núcleo. Para adicionar outra ação, arraste-a para o poços **Ações** na parte inferior da página.



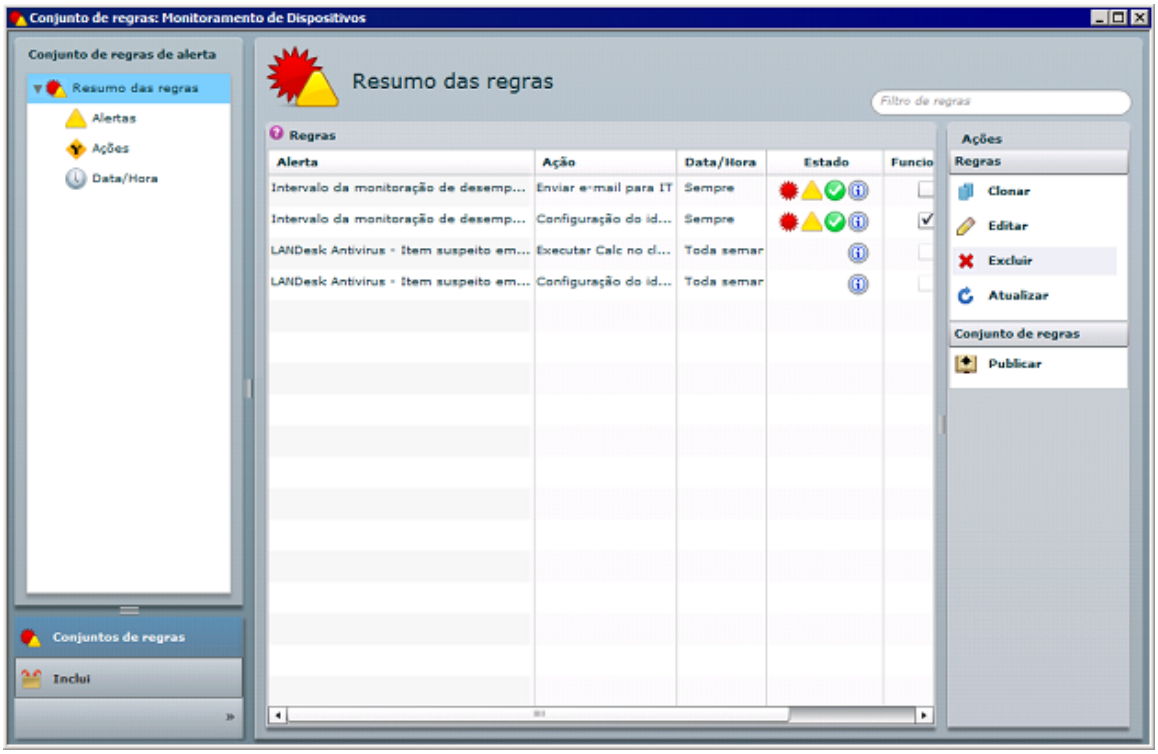
A pasta **Padrão** contém ações pré-definidas. Para usar outro tipo de ação, você precisa definir a ação primeiro.

6. Clique em **Tempo** para especificar a freqüência com que o alerta deve ser monitorado. Arraste uma regra de tempo (por exemplo, **Sempre**) para o poço **Tempo** na parte inferior da página.



Como padrão, existem três regras de tempo disponíveis. Você também pode definir diferente regras de tempo se necessário.

7. Quando você tiver pelo menos um alerta com uma ação e tarefa de tempo associada, clique no botão **OK** na parte inferior da página para adicionar a regra de alerta ao conjunto de regras. Clique em **OK** novamente.
8. Na coluna da direita, clique no botão **Publicar**.
9. Na coluna da esquerda, clique em **Resumo de regras** para ver o conjunto de regras atualizado com novos alertas.



Com uma lista dos alertas no conjunto de regras, você pode editar cada item para alterar a ação e o tempo associados. Você pode também selecionar quais níveis de severidade aplicar ao alerta e especificar se o alerta deve contribuir para o funcionamento do dispositivo.

Detalhes sobre definição de ações e filtros de tempo, edição de propriedades de regra são encontrados nos tópicos a seguir.

Definir ou editar um Alerta de monitoramento

Defina um alerta na seção de Monitoramento de alertas e você poderá editar um Alerta de monitoramento existente (por exemplo: para mudar as frequência da sondagem).

1. Na coluna esquerda da página do **Conjunto de regras de alerta**, clique em **Alertas**.
2. No modo de exibição de árvore, role para seção de **Monitor.** Você pode criar ou editar um alerta somente no Cabeçalho do monitor.
3. Selecionar uma categoria (for exemplo, **Chassi**), depois clique em **Tarefas > Novo** na coluna da direita.
4. Adicionar informações nos campos **Nome**, **Descrição**, e **Intervalo de sondagem** quando necessário, depois clique em **OK**.

O alerta está listado na categoria selecionada e está disponível para ser adicionada ao conjunto de regras.

Definir as ações de alerta a serem usadas nas regras

1. Na coluna da esquerda da página **Conjunto de regras de alerta**, clique em **Ações**.
2. Selecione um grupo de ação (por exemplo, **Enviar e-mail**) e clique em **Tarefas > Nova** na coluna da direita.
3. Adicione as informações nos campos e clique em **Salvar**.

A ação está listada no grupo selecionado e disponível para ser associada aos alertas. Detalhes sobre os campos em diferentes tipos de ações são explicados abaixo.

Executar no núcleo/Executar no cliente

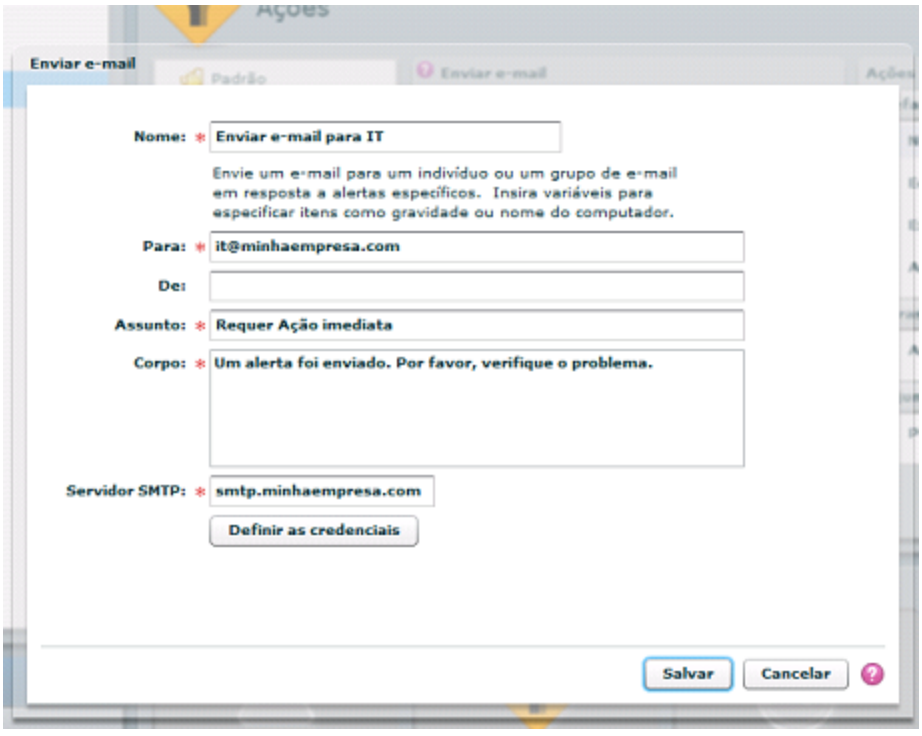
Esta ação inicia um arquivo executável tanto no servidor núcleo como no dispositivo gerenciado.

- **Nome**: o nome de identificação para a ação. Seja específico para que possa distinguir as ações facilmente.
- **Caminho e norme do arquivo**: o caminho completo e o nome do arquivo para o executável a ser executado no servidor núcleo ou no dispositivo gerenciado. Ao disparar o alerta, o agente de alerta enviará um comando para executar esse arquivo.

Ao selecionar ambas ações, note que os programas podem não ser mostrados como o esperado no desktop. Quando o programa é executado, ele é iniciado em Windows e, assim, ele não é mostrado da forma como um aplicativo normal é exibido. Os programas que são executados dessa forma não devem conter interface de usuário que requer interação. Para determinar se o programa foi realmente executado, verifique os processos no Gerenciador de tarefas do Windows.

Enviar e-mail

Esta ação envia uma mensagem de e-mail usando o servidor SMTP que você especificou.


Enviar e-mail
Nome: * Enviar e-mail para IT
Envie um e-mail para um indivíduo ou um grupo de e-mail em resposta a alertas específicos. Insira variáveis para especificar itens como gravidade ou nome do computador.
Para: * it@minhaempresa.com
De:
Assunto: * Requer Ação imediata
Corpo: * Um alerta foi enviado. Por favor, verifique o problema.
Servidor SMTP: * smtp.minhaempresa.com
Definir as credenciais
Salvar
Cancelar

- **Nome**: o nome de identificação para a ação. Seja específico para que possa distinguir as ações facilmente.
- **Para**: o endereço de e-mail completo da pessoa que você deseja que receba a notificação por e-mail.
- **De**: um endereço de e-mail válido, preferivelmente um que indique que o e-mail é uma notificação de alerta. Se não for um e-mail válido, a mensagem não será enviada.
- **Assunto**: um assunto descritivo para o e-mail de notificação.
- **Corpo:** uma mensagem que acompanha a notificação de alerta.
- **Servidor SMTP**: o local de um servidor SMTP de onde o e-mail pode ser enviado.
- **Definir credenciais**: clique para especificar um nome de usuário e senha que possam ser usados para efetuar logon no servidor SMTP.

O e-mail será enviado a partir do servidor núcleo.

Você pode enviar mensagens de e-mail para vários destinatários e pode usar as seguintes variáveis no campo Corpo:

- %% = %
- %D = Descrição
- %N = Nome do computador
- %S = Severidade
- %T = Hora (UTC)

Enviar interceptação SNMP

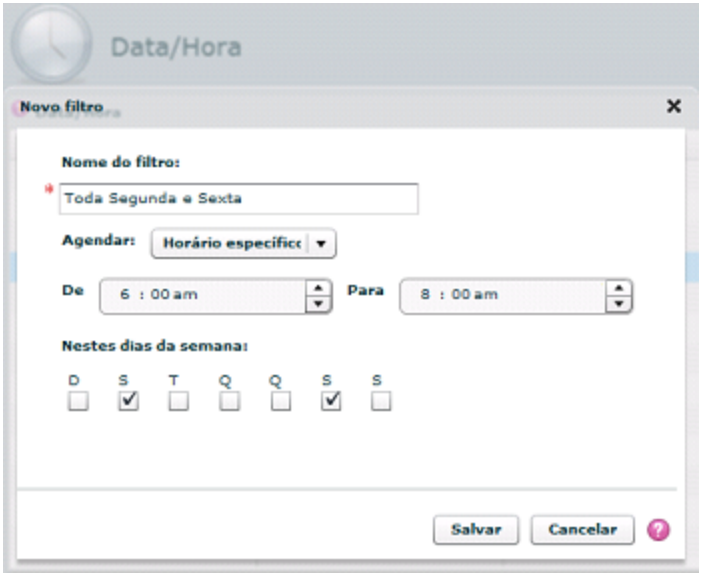
Esta ação envia uma interceptação SNMP v1 quando o alerta é disparado.

- **Nome**: o nome de identificação para a ação. Seja específico para que possa distinguir as ações facilmente.
- **Nome do host**: o nome do host SNMP que receberá a interceptação.
- S**tring de comunidade**: uma string da comunidade v1 usada pelo host para receber interceptações.

Os níveis de severidade para os alertas são reportados no campo Tipo específico de interceptação da interceptação. Os valores são 1 = desconhecido, 2 = informacional, 3 = OK, 4 = aviso, 5 = crítico.

Definir os filtros de tempo a serem usado nas regras de alerta

1. Na coluna da esquerda da página **Conjunto de regras de alerta**, clique em Tempo.
2. Clique em **Tarefas > Nova** na coluna da direita.
3. Na caixa de diálogo **Novo filtro**, digite os dados nos campos (descrito abaixo).
4. Clique em **Salvar**.



O filtro de tempo aparece na lista e está disponível para ser associado aos alertas. Os campos na caixa de diálogo **Novo filtro** incluem:

- **Nome do filtro**: o nome identificador do filtro.
- **Agenda**: seleciona a **Hora específica** para um filtro que limita o tempo e os dias quando o alerta é monitorado. Selecione **Qualquer hora** para monitorar o alerta continuamente.
- **De** e **Para**: selecione uma hora de início e de término durante o dia quando o alerta é monitorado.
- **Neste dias da semana**: selecione os dias em que você quer que o alerta seja monitorado.

Editar uma regra de alerta

Você pode editar as regras de alerta individualmente na página **Resumo de regras**. As alterações que podem ser feitas incluem a seleção de uma ação ou filtro de tempo diferentes, a seleção de quais níveis de severidade estão ativos e a especificação se a regra contribui para o status de funcionamento do dispositivo.

1. Clique em **Resumo de regras** para visualizar as regras de alerta no conjunto de regras atual.
2. Clique na regra de alerta que deseja editar e clique em **Regras > Editar** na coluna da direita.
3. Para alterar a ação ou tempo associado, selecione uma nova opção a partir da lista respectiva.
4. Para receber uma notificação de alerta somente para níveis de severidade em participar, clique nos ícones de **Estado**. Um ícone esmaecido indica que aquele alerta para aquele nível de severidade será ignorado.
5. Para incluir a regra de alerta como um indicador de funcionamento do dispositivo, marque a caixa de seleção **Funcionamento**.
6. Clique em **OK** para salvar suas mudanças.

Clonar uma regra de alerta

Cara regra de alerta pode ter apenas uma ação associada e um filtro de tempo. Se deseja criar regras adicionais para um alerta, clique em **Clonar** na coluna da direita para duplicar uma regra e editar a duplicada.

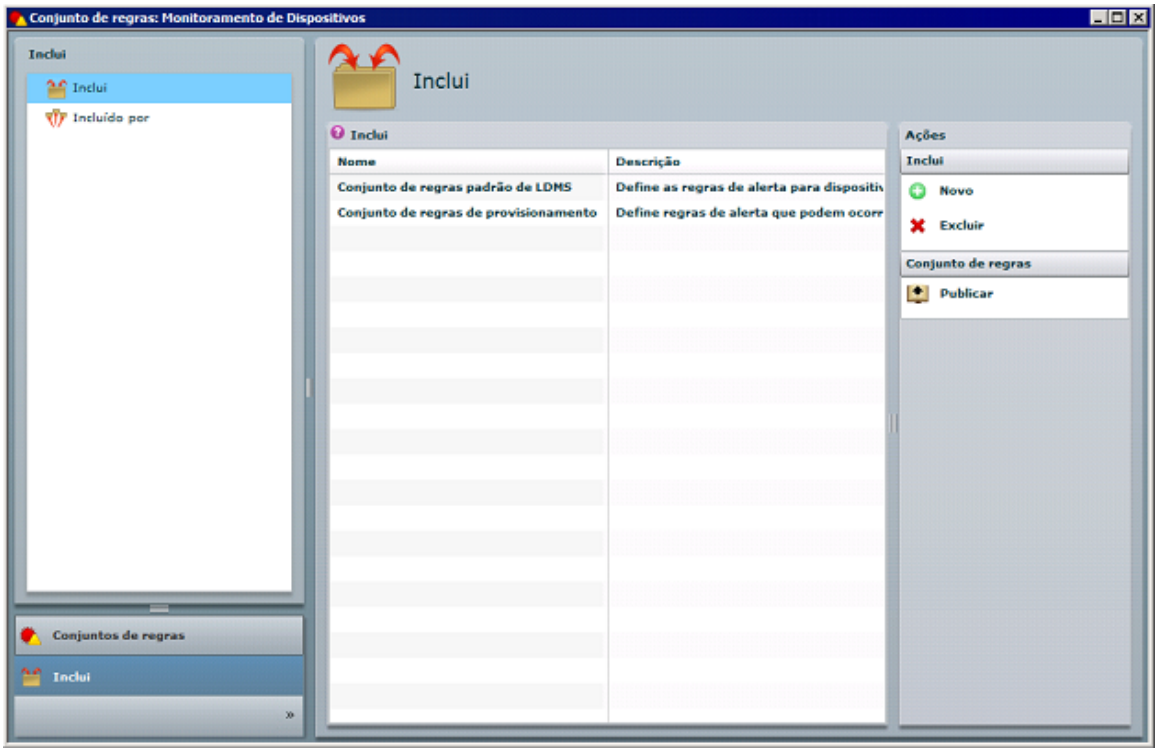
Incluir conjuntos de regras com outros conjuntos de regras

Um meio de tornar a criação de conjunto de regras mais flexível é criar conjuntos de regras menores que podem ser combinados em diferentes usos. Para tanto, você pode incluir conjuntos de regras com outros conjuntos de regras.

1. Na parte inferior esquerda da página **Conjunto de regras de alerta**, clique em **Inclui**.
2. Na coluna esquerda, clique em **Inclui**.
3. Na coluna da direita, clique em **Inclui > Nova**.
4. Na caixa de diálogo **Conjuntos de regras disponíveis**, selecione um ou mais conjuntos de regras para incluir no conjunto de regras atual e clique em **Salvar**. Use Ctrl+clique ou Shift+clique para selecionar vários conjuntos de regras.

   Os conjuntos de regras são adicionados à lista **Inclui**.

5. Se deseja remover um conjunto de regras da lista **Incluir**, selecione-o e clique em **Inclui > Excluir** na coluna da direita.
6. Para ver quais outros conjuntos de regras incluem o conjunto de regras atual, clique em **Incluído por** na coluna da direita.



Ao incluir os conjuntos de regras, cada conjunto de regra individual é mantido como um arquivo XML individual. Os arquivos XML não são combinados, mas fazem referência uns aos outros

Publicar um conjunto de regras de alerta

Depois de ter adicionado e editado regras em um conjunto de regras, você precisa publicar o conjunto de regras. Isso cria um arquivo XML com os dados do conjunto de regras relacionados pelo agente de alerta conforme ele trabalha.

1. Na página **Resumo de regras**, clique em **Publicar** na coluna direita.
2. Clique em **OK** na mensagem de operação bem sucedida.

Os arquivos XML com os dados do conjunto de regras publicados estão armazenados no compartilhamento ldlogon no servidor núcleo, na pasta alertrules.

Ao publicar um conjunto de regras, o serviço de alerta é notificado para recarregar o conjunto de regras atualizado. Ao atualizar o conjunto de regras já distribuído para os dispositivos gerenciados, cada um desses dispositivos irá automaticamente atualizar seus conjuntos de regras na próxima vez que o agente de alerta for executado neles.

Se você não publicar o conjunto de regras, não haverá sinal para o serviço de alerta recarregar o conjunto de regras e não haverá atualização automática do conjunto de regras nos dispositivos que já possuem conjunto de regras. É altamente recomendado que você publique os conjuntos de regras cada vez que fizer alterações neles.

Sobre o desempenho do monitoramento

O Management Suite oferece vários métodos de monitoramento do funcionamento de um dispositivo. Enquanto os conjuntos de regras de alerta são definidos no console do núcleo e distribuídos para vários dispositivos, nos dispositivos individuais você também pode definir os contadores de monitoração de desempenho para monitorar questões específicas de desempenho.

Você pode definir contadores de desempenho e monitorá-los para vários tipos de dados nos seus dispositivos, tais como:

- Componentes de hardware (tais como unidades de disco, processadores e memória)
- Sensores de hardware (ventiladores, voltagens e temperatura)
- Componentes de SO (tais como processos e serviços)
- Componentes de aplicativos (tais como bytes por segundo transferidos pelo servidor Web do sistema)
- Níveis de utilização

Quando um contador de desempenho é selecionado, você especifica a freqüência da sondagem do item e também especifica os limites de desempenho e o número de violações a serem permitidas antes de ser gerado uma alerta. Depois de definir um contador de desempenho, você pode abrir a página de **Monitoramento** no console de Inventário e monitoramento em tempo real e ver um sumário de seus alertas monitorados.

Para ser alertado sobre os itens de monitoração de desempenho em um dispositivo, você deve incluir uma regra de monitoração de desempenho no conjunto de regras para aquele dispositivo.

Processos para monitoramento de itens de desempenho em dispositivos

Para monitorar o desempenho de diversos itens em seus dispositivos gerenciados, execute as três tarefas gerais a seguir:

- Instalação de um agente de monitoramento em dispositivos
- Criação de regras de monitoramento de desempenho para dispositivos individuais
- Visualização dos dados de monitoramento de desempenho

Notas

- Se desejar apenas fazer ping regularmente nos dispositivos para monitorar a conectividade deles, use o recurso de monitoração de dispositivo.
- As comunicações com o agente de monitoramento são feitas via HTTP sobre TCP/IP no formato de solicitações GET ou POST. As respostas às solicitações são feitas em documentos XML.
- Ao executar e armazenar uma consulta sobre o status de funcionamento de dispositivos (Computer.Health.State), o estado no banco de dados é representado por um número. Os números correspondem aos seguintes estados: 4=Crítico, 3=Advertência, 2=Normal, 1=Informativo, nulo ou 0=Desconhecido.
- O monitoramento de hardware depende dos recursos do hardware instalado em um dispositivo, assim como da correta configuração do hardware. Por exemplo, se um disco rígido com recurso de monitoração S.M.A.R.T. for instalado em um dispositivo e a detecção S.M.A.R.T. não for habilitada nas configurações do BIOS do dispositivo, ou se o BIOS do dispositivo não oferecer suporte a unidades S.M.A.R.T., os dados de monitoração não estarão disponíveis.
- Se estiver fazendo um relatório de um computador específico que parece ter travado, você poderá usar o restartmon.exe na pasta LDCLIENT para reiniciar o coletor e todo os provedores de monitoração. Esse utilitário destina-se a computadores em que a geração de relatórios foi instalada e parou de funcionar. Use-o para reiniciar o coletor e os provedores sem ter que reinicializar o dispositivo.

Tópicos relacionados

"Noções básicas sobre alertas" na página 793

"Monitoramento de dispositivos para conectividade de rede" na página 792

Distribuir um agente de monitoramento nos dispositivos

O Management Suite oferece um resumo imediato da condição de um dispositivo quando o agente de monitoramento é instalado no dispositivo. O agente de monitoramento é um dos componentes do agente que podem ser instalados em dispositivos gerenciados.

O Inventário e monitoramento em tempo real verifica o hardware e a configuração do dispositivo de forma regular e periódica e reflete quaisquer alterações em seu status de funcionamento. O status do dispositivo é exibido em três lugares:

- O ícone status nas listas **Dispositivos** no modo de exibição de rede
- O status de funcionamento exibido no Dashboard de funcionamento (clique em **Ferramentas > Relatórios/Monitoramento > Dashboard de funcionamento**).
- Dados exibidos no dashboard do Inventário e monitoração em tempo real (clique com o botão direito na tela de rede e selecione **Inventário e monitoramento em tempo real**)

Por exemplo, um dispositivo monitorado que possui um disco rígido cujo espaço está se esgotando poderá mostrar um ícone de status de advertência quando o disco atingir 90% da capacidade total e que será alterado para um ícone de status crítico quando o disco atingir 95% da capacidade total. Você também poderá receber alertas para o status do mesmo disco rígido se o dispositivo possuir um conjunto de regras de alerta que inclua regras de monitoramento de desempenho para um disco.

Tópicos relacionados

Configuração de agentes de dispositivo

Criação de regras de monitoramento de desempenho

Você pode escolher quais itens de desempenho são monitorados em um dispositivo definindo regras de monitoramento que especificam o que o agente de monitoramento deve verificar no dispositivo. Para isso, você precisa distribuir um conjunto de regras para o dispositivo que inclui a regra de alerta de monitoração de desempenho.

Existem vários contadores de desempenho que podem ser monitorados. Ao criar uma regra de monitoramento de desempenho, você poderá ativar ou desativar qualquer um desses itens, especificar a freqüência na qual deseja que eles sejam verificados e definir os limites de desempenho para alguns itens. É possível também selecionar serviços em execução nos dispositivos que deseja monitorar.

O processo geral para a criação de regras de monitoramento de desempenho é o seguinte:

1. Incluir a monitoração de desempenho como uma regra no conjunto de regras de alerta para o dispositivo.
2. Distribuir o conjunto de regras de alerta para o dispositivo. (Você pode definir vários dispositivos para distribuir o conjunto de regras para vários dispositivos, mas precisa definir a monitoramento de desempenho em dispositivos individuais.)
3. Cria regras de monitoramento no dispositivo usando o console de Inventário e monitoramento em tempo real. Alguns eventos, como serviços, também necessitam que você selecione cada serviço que você quer monitorar (passos detalhados abaixo).

Para selecionar um contador de desempenho a monitorar

1. Clique em **Ferramentas > Relatórios/Monitoramento > Dashboard funcionamento**.
2. Na lista de dispositivos, clique duas vezes no dispositivo que deseja configurar.
   O console de Inventário e monitoramento em tempo real abre em outra janela do navegador.
2. No painel de navegação esquerdo, clique em **Monitoramento**.
3. Clique na guia **Configurações do contador de desempenho**.
4. Na coluna **Objetos**, selecione o objeto que deseja monitorar.
5. Na coluna **Instâncias**, selecione a instância do objeto que deseja monitorar, se aplicável.
6. Na coluna **Contadores**, selecione o contador específico que deseja monitorar.
2. Se o contador desejado não aparecer na lista, clique em **Recarregar contadores** para atualizar a lista com quaisquer objetos, instâncias ou contadores.
7. Especifique a frequência de sondagem (polling) (**a cada*n* segundos**) e o número de dias em que o histórico deverá ser mantido.
8. No campo **Alertar após o contador estar fora do intervalo**, especifique o número de vezes que o contador poderá ultrapassar o limite antes de ser gerado um alerta.
9. Especifique os limites superior e/ou inferior.
10. Clique em **Aplicar**.

Notas

- Os arquivos de log de desempenho podem tornar-se grandes demais, rapidamente. A sondagem de um único contador em intervalos de dois segundos adiciona 2,5 MB de informações ao log de desempenho diariamente.
- Um alerta de advertência é gerado quando um contador de desempenho vai abaixo do limite mais baixo em um dispositivo Windows ou Linux. Quando um contador de desempenho excede o limite mais alto em um dispositivo Linux, é gerado um alerta de advertência. Quando um contador de desempenho excede o limite mais alto em um dispositivo Windows, é gerado um alerta crítico.
- Na configuração dos limites, lembre-se de que serão gerados alertas independentemente do limite ultrapassado, superior ou inferior. No caso de espaço em disco, por exemplo, você talvez queira ser alertado somente se o dispositivo estiver sendo executado muito baixo. Nesse caso, é aconselhável configurar o limite maior a um número alto o suficiente para que você não receba um alerta se uma quantidade grande do espaço em disco tornar-se disponível no dispositivo.
- Mudar o número em **Alertar após o contador estar fora do intervalo** lhe permite focar em um problema quando ele é persistente ou quando ele é um evento isolado. Por exemplo, se você estiver monitorando os bytes enviados de um servidor Web, o Management Suite pode alertá-lo quando a quantidade de bytes/seg. estiver consistentemente alta. Ou você pode especificar um número baixo, como 1 ou 2, para ser alertado sempre que o número de conexões anônimas de FTP exceder um certo número de usuários.
- Quando os serviços são editados em uma regra de monitoramento, a lista **Serviços disponíveis** mostra os serviços conhecidos do banco de dados de inventário. Nenhum serviço será exibido na caixa de listagem **Serviços disponíveis** até que um agente LANDesk tenha sido distribuído para um ou mais dispositivos e uma análise de inventário seja retornada ao núcleo. Por exemplo, para selecionar serviços Linux na lista, é necessário primeiro distribuir um agente para o dispositivo Linux.

Gerar um arquivo XML par um conjunto de regras

Como parte do processo de distribuição, é criada uma página em XML contendo os conjuntos de regras distribuídos e os dispositivos para os quais os conjuntos de regras foram distribuídos. Este relatório é gravado no servidor núcleo no diretório LDLOGON e é nomeado com um número sequencial atribuído pelo banco de dados.

Para ver essa página XML separadamente da distribuição de um conjunto de regras, clique no botão **Gerar XML** e clique no link para ver o arquivo XML. A geração de um conjunto de regras também permite que ele seja mostrado na lista de conjuntos de regras disponíveis nas definições da **Configuração de agentes**.

Visualização dos dados de monitoramento de desempenho

A página **Monitoramento** permite monitorar o desempenho de vários objetos do sistema. É possível monitorar componentes de hardware específicos, como unidades, processadores e memória, ou monitorar componentes do SO, como processos ou bytes por segundo transferidos pelo servidor Web do sistema. A página **Monitoramento** inclui um gráfico que mostra os dados em tempo real ou os dados históricos de contadores.

Para monitorar um contador de desempenho, primeiramente selecione o contador. Isto o adicionará à lista de contadores monitorados. Quando você faz isso, você também especifica a freqüência da sondagem do item e especifica os limites de desempenho e o número de violações a serem permitidas antes de ser gerado uma alerta.

Para ver contadores de desempenho monitorado

1. Clique em **Ferramentas > Relatórios/Monitoramento > Dashboard funcionamento**.
2. Na lista de dispositivos, clique duas vezes no dispositivo que deseja configurar.
   O console de Inventário e monitoramento em tempo real abre em outra janela do navegador.
2. Na caixa de ferramentas, clique em **Monitoramento**.
3. Clique na guia **Contadores de desempenho ativos**, se necessário.
4. Na lista suspensa **Contadores**, selecione o contador do qual deseja ver um gráfico do desempenho.
5. Selecione **Visualizar dados em tempo real** para exibir um gráfico de desempenho em tempo real.
6. Para exibir um gráfico exibindo o desempenho durante um período de tempo, selecione **Visualizar dados históricos** (Manter histórico) ao selecionar o contador.

Notas

No gráfico de desempenho, o eixo horizontal representa o tempo decorrido. O eixo vertical representa as unidades sendo medidas, como bytes por segundo (ao monitorar transferências de arquivos, por exemplo), Porcentagem (ao monitorar a porcentagem de CPU em uso) ou bytes disponíveis (ao monitorar o espaço em discos rígidos). A altura da linha não é uma unidade fixa. A altura da linha muda com relação aos valores extremos dos dados; para um contador o eixo vertical pode representar 1 a 100, e para outro ele pode representar 1 a 500.000. Quando os dados variam entre extremos amplos, mudanças mínimas podem ser exibidas como uma linha reta.

Contadores monitorados são relacionados com colunas para indicar a frequência com que são verificados, número de vezes que o contador está fora do intervalo para um alerta ser enviado e as configurações de limites superior e inferior.

A seleção de outro contador atualiza o gráfico e redefine as unidades de medida.

Se receber um alerta gerado por um contador na lista, clique com o botão direito do mouse no contador e clique em **Reconhecer** para limpar o alerta.

Para o monitoramento de um contador de desempenho

1. Clique em **Ferramentas > Relatórios/Monitoramento > Dashboard funcionamento**.
2. Na lista de dispositivos, clique duas vezes no dispositivo que deseja configurar. O console de Inventário e monitoramento em tempo real abre em outra janela do navegador.
2. Na caixa de ferramentas, clique em **Monitoramento**.
3. Clique na guia **Contadores de desempenho ativos**, se necessário.
4. Em **Contadores de desempenhos monitorados**, clique com o botão direito do mouse no contador e clique em **Excluir**.

Exibir o log de alertas globais

Use a página **Log de alertas** para ver os alertas enviados para o servidor núcleo. O log é ordenado pela hora (GMT) com o alerta mais recente na parte superior do log.

Para ver o log de alertas globais

1. Clique em **Ferramentas > Relatórios/Monitoração > Logs**.
2. Para ordenar as entradas por coluna, clique em um cabeçalho de coluna.

3. Para ver uma descrição mais detalhada do alerta, clique duas vezes na entrada, na coluna **Nome do alerta**.
4. Para mostrar as entradas por nome, status ou exemplo, selecione o critério de filtro na lista suspensa **Filtro**. Por exemplo, selecione **Nome do alerta** e digite um nome completo (por exemplo, Desempenho) ou um nome parcial com o caractere curinga * (por exemplo, Remoto*) na caixa **Buscar**. Para fazer uma busca por data, selecione **Habilitar filtro de data**, insira uma faixa de datas com uma data inicial e outra final. Ao adicionar critérios de filtro, clique no botão **Pesquisar**.
5. Para limpar o status de funcionamento de um alerta, selecione o alerta na coluna **Nome do alerta**, clique no botão **Reconhecimento** na barra de ferramentas e clique em **OK**.
6. Para excluir uma entrada de log, clique com o botão direito no alerta e selecione **Excluir**.

NOTA: Se o nome do dispositivo não for mostrado como um nome de domínio totalmente qualificado, é porque este produto não conseguiu resolvê-lo para o dispositivo.

Clique aqui para ver as descrições das colunas de log de alertas.

- **Nome do alerta:** O nome associado ao alerta, conforme definido na página **Configurações de alerta**.
- **Hora GMT:** A data e a hora em que o alerta foi gerado (GMT).
- **Status:** O status de gravidade do alerta, que pode ser um dos seguintes:
  - **Desconhecido:** O status não pode ser determinado.
  - **Informativo:** Suporta mudanças de configuração ou eventos que os fabricantes incluem em seus sistemas.
  - **OK:** Indica que o status é um nível aceitável.
  - **Aviso:** Fornece algum tipo de advertência antecipada de um problema antes deste atingir um ponto crítico.
  - **Crítico:** Indica que o problema precisa de atenção imediata.
- **Nome do dispositivo:** O nome do dispositivo no qual o alerta foi gerado. Este deve ser um nome de domínio totalmente qualificado.
- **Endereço IP:** O endereço IP do dispositivo no qual o alerta foi gerado.
- **Instância:** Fornece mais informações detalhadas conforme a situação na qual o alerta foi gerado.

Exibir o log de alerta de um dispositivo

Use a página **Log de alertas** para exibir os alertas enviados para um dispositivo gerenciado. O log é ordenado pela hora (GMT) com o alerta mais recente na parte superior do log.

Para ver o log de alertas de um dispositivo específico

1. Clique em **Ferramentas > Relatórios/Monitoração > Dashboard de funcionamento**.
2. Na lista de dispositivos, clique duas vezes em um dispositivo.
3. No painel de navegação esquerdo, clique em **Informações do sistema**.
3. Clique em **Logs > Log de alerta**.
4. Para ordenar entradas por hora, nome ou status, clique em um cabeçalho de coluna.
5. Para ver uma descrição mais detalhada do alerta, clique duas vezes na entrada, na coluna **Nome do alerta**.

6. Para mostrar as entradas de log por nome ou status, clique no botão **Filtrar** na barra de ferramentas e selecione os critérios de filtro. Por exemplo, selecione **Nome do alerta** e digite um nome completo (por exemplo, Desempenho) ou um nome parcial com o caractere curinga * (por exemplo, Remoto*). Para fazer uma busca por data, selecione **Habilitar filtro de data**, insira uma faixa de datas com uma data inicial e outra final. Depois de adicionar o critério de filtro, clique em **Buscar.**
7. Para limpar o status de funcionamento de um alerta, selecione o alerta na coluna **Nome do alerta**, clique em **Reconhecimento de alertas** na barra de ferramentas e clique em **OK**.
8. Para excluir uma entrada de log, clique no alerta na coluna **Nome do alerta** e clique em **Excluir entrada** na barra de ferramentas.

Você também pode visualizar o alerta do dispositivo de log clicando no botão **Log de alerta** na página **Conjunto de regras** no console de inventário e monitoramento em tempo real.

NOTA: Se o nome do dispositivo não for mostrado como um nome de domínio totalmente qualificado, é porque este produto não conseguiu resolvê-lo para o dispositivo.

Clique aqui para ver as descrições das colunas de log de alertas.

- **Nome do alerta:** O nome associado ao alerta, conforme definido na página **Configurações de alerta**.
- **Hora GMT:** A data e a hora em que o alerta foi gerado (GMT).
- **Status:** O status de gravidade do alerta, que pode ser um dos seguintes:
  - **Desconhecido:** O status não pode ser determinado.
  - **Informativo:** Suporta mudanças de configuração ou eventos que os fabricantes incluem em seus sistemas.
  - **OK:** Indica que o status é um nível aceitável.
  - **Aviso:** Fornece algum tipo de advertência antecipada de um problema antes deste atingir um ponto crítico.
  - **Crítico:** Indica que o problema precisa de atenção imediata.
- **Instância:** Fornece mais informações detalhadas conforme a situação na qual o alerta foi gerado.

Monitoramento do conteúdo dos arquivos de log

A Monitoração de arquivos de log é uma opção disponível nas regras de monitoração de desempenho. O agente de monitoração analisa os arquivos de log nos dispositivos Windows gerenciados em busca de seqüências de caracteres ou expressões específicas e gera alertas ao encontrá-las. Isso é útil se você deseja ser alertado sobre condições específicas que podem ser rastreadas por meio de arquivos de log.

Você pode monitorar arquivos de texto gerados por qualquer aplicativo, incluindo arquivos .htm e .xml (com exceção de arquivos Unicode). Após especificar o arquivo que será monitorado e definir as regras usando expressões regulares, o arquivo será monitorado enquanto as regras de monitoramento de um arquivo de log contidas em um conjunto de regras estiver em vigor no dispositivo em questão.

Na primeira vez que um trecho de texto no arquivo de log corresponder a uma expressão regular, um alerta será gerado. O alerta será gerado somente uma vez para o arquivo, mesmo se houver várias correspondências. Posteriormente, se o arquivo sofrer alguma alteração a ponto de não haver mais uma condição de correspondência, o assistente começará a procurar a expressão regular novamente e gerará outro alerta ao encontrar a próxima correspondência.

Você pode também analisar os arquivos de backup de log criados quando um arquivo de log se torna muito grande, fazendo com que as entradas mais antigas no arquivo sejam adicionadas a um arquivo diferente (um arquivo de log "deslocável"). No entanto, não há suporte para arquivos de log "empacotados", que removem as entradas mais antigas em um único arquivo de log para liberar espaço para novas entradas).

Para esta opção de monitoramento, você deve especificar o local e o nome exato do arquivo no dispositivo gerenciado, além dos critérios de pesquisa por meio de uma expressão regular. Quando uma seqüência de caracteres no arquivo atender à expressão, uma ação de alerta será gerada se você tiver definido um tipo de alerta da **Monitoração de arquivos de log** no conjunto de regras de alerta apropriado.

Você pode incluir a monitoração de arquivos de log em qualquer conjunto de alertas definido. O prosseguimento a seguir descreve as cinco etapas gerais para a configuração da monitoração de arquivos de log:

1. Criar uma regra de monitoramento de arquivo de log em um conjunto de regras de alerta
2. Especificar quais os arquivos que devem ser monitorados nos dispositivos gerenciados.
3. Definir as regras de monitoramento para aquele arquivo, usando expressões regulares
4. Selecionar um nível de severidade e nomeie a instância para que seja identificada nos alertas.
5. Aplicar regras de ação e tempo e salvar a regra no conjunto de regras de alerta

Notas

- O monitoramento de arquivo de log é suportada somente para dispositivos gerenciados Windows.
- Sempre que editar ou excluir uma regra, será necessário publicar o conjunto de regras de alerta em que a regra aparece. As alterações feitas não serão aplicadas aos dispositivos até que o conjunto de regras seja publicado (ou até que você redistribua o conjunto de regras com uma tarefa agendada).
- Este recurso mapeia os arquivos de log na memória para usar menos memória durante uma pesquisa. Memória de tempo de execução é alocada para este processo à medida que pesquisas de expressões regulares ocorrem. Como o Windows bloqueia os arquivos mapeados na memória, poderá haver problemas com alguns aplicativos.

Tópicos relacionados

"Configuração de conjunto de regras de alerta" na página 799

"Para configurar uma regra de monitoramento de arquivos de log" na página 819

Para configurar uma regra de monitoramento de arquivos de log

1. Clique em **Ferramentas > Configuração > Alerta**.
2. Em **Conjunto de regras de alerta**, selecione o conjunto de regras que deseja editar e clique em **Editar** na barra de ferramentas.
3. Na coluna da esquerda, na janela **Conjunto de regras de alerta** que se abrirá, clique em **Alertas**. Na pasta **Monitor** na lista de alertas, clique em **Monitoramento de arquivos de log**.
4. Clique em **Tarefas > Nova** na coluna da direita.
5. Na caixa de diálogo **Monitoramento de arquivo de log** digite um nome e uma descrição para a regra de monitoramento de arquivo de log.
6. Para alterar a freqüência na qual um item é monitorado, altere as configurações **Intervalo de sondagem**.

7. Clique em **Configuração do arquivo de log** para especificar quais arquivos de log serão monitorados, o que você está monitorando e como será alertado.
   Expressões regulares são usadas para definir qual o conteúdo no arquivo de log deve ser monitorado. Quando o serviço de monitoramento encontra um correspondente para a expressão regular no arquivo de log, ele segue as regras de alerta para notificá-lo da ocorrência.
8. Clique em **Gerenciar**. Na caixa de diálogo **Gerenciamento de expressões regulares**, adicione um nome descritivo e uma expressão regular e clique em **Adicionar**. Repita o procedimento para cada expressão regular que você desejar utilizar para monitoramento dos arquivos de log. Após adicionar todas, clique em **OK**.
   Você pode adicionar quantas expressões regulares desejar nesta caixa de diálogo. Observe que você precisa criar uma nova regra para cada expressão que deseja pesquisar e cada regra é aplicada em um único arquivo de log. Em outras palavras, cada regra inclui uma expressão regular e um arquivo de log.
9. Selecione uma expressão regular na lista suspensa **Expressão regular**.
10. Digite o caminho e preencha o nome de arquivo do arquivo de log que deseja monitorar na caixa **Caminho do arquivo de log**. Deve ser um nome de arquivo específico e somente ele será monitorado (por exemplo, c:\logs\error.txt)
11. Para incluir arquivos de backup para o arquivo de log, insira o caminho e o nome completos do arquivo de backup na caixa **Arquivo de log de backup** (esta etapa é opcional). Isso também é necessário para completar o caminho e o nome de arquivo para um arquivo específico.
12. Digite um nome descritivo de **Instância** . Isso identifica a regra de monitoramento de arquivo de log nas notificações de alerta que você receber.
13. Selecione o nível de severidade que deseja aplicar a esta regra de alerta.
14. Se desejar monitorar somente novas entradas no arquivo de log (começando quando a regra de monitoramento é distribuída ao dispositivo), clique em **Alterações de monitoramento para os arquivos de log**. (Esta opção é normalmente usada para arquivos de log para que o agente não continue analisando o mesmo texto existente.)
    Para monitorar todas as entradas novas e existentes no arquivo de log, clique em **Monitorar o arquivo de log inteiro**. (Esta opção é usada tipicamente para monitorar outros arquivos menos dinâmicos, tais como arquivos de configuração.)
15. Clique em **OK** para adicionar a regra à lista de regras de monitoramento de arquivos de log.
16. Repita os passos 4 à 15 para adicionar outras regras de monitoramento de arquivos de log.
    Depois de criar as regras de monitoramento de arquivos de log conforme desejado, você precisa adicioná-las ao conjunto de regras. Você pode adicionar várias regras de monitoramento e aplicar regras de tempo e ação nelas, dependendo de como você deseja ser notificado quando o "gatilho" de mudanças nos arquivos de log for disparado.
17. Na lista de regras em **Monitoramento de arquivo de log**, clique em **Regra > Nova**, na coluna da direita.
    Três caixas ou "compartimentos" são exibidos na parte inferior da página.
18. Arraste uma ou mais regras para a caixa **Alertas** .
19. Clique em **Ações** na coluna da esquerda e arraste uma ou mais regras de ação para a caixa **Ações** .
    As ações adicionadas aqui serão aplicadas para cada regra adicionada.
20. Clique em **Tempo** na coluna da esquerda e arraste uma regra de tempo para a caixa **Tempo** .

21. Clique em **OK** para adicionar novas regras ao conjunto de regras.
    Para exibir as novas regras de arquivo de log de monitoramento no conjunto de regras, clique em **Resumo de regras**. Cada regra é exibida em uma linha separada e você pode editar regras individuais ou clonar uma regra e fazer cópias com ações diferentes, regras de tempo ou estados de severidade. Se deseja que a regra de alerta afete o funcionamento do dispositivo, clique duas vezes na lista **Resumo de regras** e marque a caixa de seleção **Funcionamento**.
22. Depois de adicionar as regras de monitoramento de arquivo de log ao conjunto de regras, clique em **Publicar** para salvar as alterações do conjunto de regras. As alterações serão aplicadas a dispositivos individuais na próxima vez que o conjunto de regras for distribuído ou na próxima vez em que o serviço de inventário for executado.

Notas

- O monitoramento de arquivo de log é suportada somente para dispositivos gerenciados Windows.
- Sempre que editar ou excluir uma regra, será necessário publicar o conjunto de regras de alerta em que a regra aparece. As alterações feitas não serão aplicadas aos dispositivos até que o conjunto de regras seja publicado (ou até que você redistribua o conjunto de regras com uma tarefa agendada).
- Este recurso mapeia os arquivos de log na memória para usar menos memória durante uma pesquisa. Memória de tempo de execução é alocada para este processo à medida que pesquisas de expressões regulares ocorrem. Como o Windows bloqueia os arquivos mapeados na memória, poderá haver problemas com alguns aplicativos.

Configurar dispositivos Dell OMCI

Este produto inclui integração de gerenciamento com dispositivos que têm o software Dell OMCI instalado. OMCI (OpenManage Client Instrumentation) é uma tecnologia para dispositivos Dell que habilitam o gerenciamento remoto de status e configurações do dispositivo.

Quando o LANDesk Management Suite descobre um dispositivo Dell equipado com OMCI, uma ferramenta OMCI é habilitada no menu **Configurar** do console. Isso permite que você use o OMCI para mudar configurações do BIOS nos dispositivos Dell OMCI.

O processo de configuração do OMCI

Quando você abre a ferramenta de configuração do Dell OMCI, as configurações padrão que estão relacionadas são obtidas do dispositivo Dell OMCI na sua lista **Todos os dispositivos**. Se você selecionar um dispositivo primeiro, as configurações desse dispositivo serão usadas para povoar a lista de configurações do BIOS. Se você não selecionar um dispositivo, a ferramenta usa as configurações do primeiro dispositivo OMCI que encontrar.

A caixa de diálogo Configuração dos parâmetros do BIOS contém as configurações do BIOS que você pode mudar. O status atual de cada configuração é mostrada e uma coluna de **Nova configuração** deixa você selecionar diferentes configurações. Além disso, você pode mudar a senha do BIOS e a etiqueta de patrimônio do BIOS.

Após configurar esses parâmetros, eles são salvos como um pacote de software de distribuição. Você pode, então, distribuir este pacote para um ou mais dispositivos Dell OMCI que você gerencia. Os parâmetros são salvos como um agente em cada dispositivo. Com algumas configurações, você receberá alertas quando o status do dispositivo mudar.

NOTA: Se você não ver as configurações que quer mudar, pode ser que essas configurações não estavam disponíveis no dispositivo Dell OMCI que foi usado para povoar a lista. Tente selecionar um dispositivo gerenciado diferente e então clique em **Configurar > Configuração do Dell OMCI** para povoar a lista com as novas configurações.

CUIDADO: Há muitas configurações de BIOS possíveis que podem ser definidas com o uso desta ferramenta. Em alguns casos, as configurações de BIOS em um dispositivo Dell podem não estar disponíveis no BIOS de outro dispositivo. É necessário ter cuidado ao selecionar dispositivos compatíveis quando criar uma configuração Dell OMCI e distribuí-la para diferentes dispositivos. Se a configuração contiver parâmetros do BIOS incompatíveis com um dos dispositivos alvo, podem ocorrer resultados imprevisível.

Para configurar definição de OMCI para dispositivos Dell

1. Se você quiser especificar que dispositivo Dell OMCI usar para povoar a lista de configurações, selecione esse dispositivo na lista **Todos os dispositivos**.
2. Clique em **Configurar | Configuração Dell OMCI**.
3. Para aplicar apenas as configurações do BIOS que você modificar na lista, selecione **Aplicar somente configurações modificadas nos clientes alvo**. Para aplicar o conjunto inteiro de configurações do BIOS aos dispositivos alvo, selecione **Aplicar todas configurações aos clientes alvo**.
4. Na lista de configurações do BIOS, mude a configuração de cada item que deseja modificar. Na coluna **Nova configuração**, clique na seta para baixo para selecionar da lista de opções.
5. Para mudar a senha do BIOS, selecione **Configurar a senha do BIOS**. Digite a nova senha e confirme-a. Para limpar a senha do BIOS, limpe as duas caixas de texto de senha.
6. Para mudar a etiqueta de patrimônio do BIOS do dispositivo, selecione **Configurar a etiqueta de patrimônio do BIOS** e digite a nova etiqueta na caixa de texto **Etiqueta de patrimônio**.
7. Clique em **OK** para salvar a configuração.
   Um pacote de distribuição é criado com as configurações que você mudou. Para aplicar a configuração aos dispositivos Dell OMCI que você gerenciar, agende o pacote de distribuição para os dispositivos alvo.
8. Clique em **Ferramentas > Distribuição > Pacotes de distribuição**.
9. Selecione o pacote na lista **Todos os pacotes**. Ele é denominado **Configurações do BIOS OMCI - <data - hora>**.
   Você pode renomear o pacote para identificar que configurações são definidas ou para descrever os dispositivos aos quais se aplica.
10. Clique com o botão direito e selecione **Criar tarefa agendada**.
11. O pacote está relacionado na ferramenta **Tarefas agendadas**. Na tela de rede, arraste cada dispositivo Dell OMCI para o pacote OMCI.
12. Clique com o botão direito no pacote e selecione **Propriedades** para ver as propriedades do pacote.
13. Clique no **Método de entrega** e selecione **Envio** como **Tipo de entrega**, em seguida, selecione distribuição por **Envio padrão** como **Método de entrega**. Clique em **Salvar**.
14. Clique com o botão direito no pacote e selecione **Iniciar agora**.
    Conforme a tarefa de distribuição avançar, o status do pacote mudará. Quando a distribuição tiver terminado, ela mostrará o número de dispositivos que foram bem sucedidos ou que falharam na tarefa de distribuição.

Após o pacote ter sido distribuído, você pode reiniciar qualquer um dos dispositivos que reconfigurou e entrar na configuração do BIOS para verificar que as mudanças foram feitas.

Gerenciamento de dispositivos Dell DRAC

LANDesk Management SuiteEste produto inclui integração de gerenciamento com dispositivos equipados com o Dell DRAC (Remote Access Controller). O DRAC é um controlador remoto de hardware que fornece uma interface ao hardware de gerenciamento de servidor compatível com IPMI no dispositivo Dell. O DRAC tem um endereço IP, usado para identificar o dispositivo DRAC na descoberta de dispositivo e no gerenciamento do dispositivo.

Os dispositivos que contêm um Dell DRAC podem ser gerenciados com a mesma funcionalidade como outros dispositivos compatíveis com IPMI. Quando o dispositivo é descoberto e adicionado à lista de dispositivos gerenciados, ele é gerenciado como qualquer outro dispositivo IPMI. Além disso, o Management Suite tem recursos Dell DRAC exclusivos.

O OpenManage Server Administrator é um console baseado na Web fornecido pela Dell para o gerenciamento do dispositivo Dell DRAC. Ele é normalmente acessado digitando-se o endereço IP do DRAC em um navegador e fazendo-se login com nome de usuário e senha. Quando um dispositivo Dell DRAC é gerenciado com o Management Suite, também é possível abrir esse utilitário diretamente da interface do Management Suite.

Além disso, o Management Suite permite o gerenciamento de nomes de usuários e senhas para acesso ao OpenManage Server Administrator e mostra três logs desse utilitário no console de informações do servidor.

Para abrir o OpenManage Server Administrator para um dispositivo Dell DRAC

1. Na tela de rede do Management Suite, clique com o botão direito no dispositivo Dell DRAC e selecione **Inventário e monitoramento em tempo real**.
2. No console de inventário de tempo real, expanda **Hardware** e clique em **Dell DRAC**. O endereço IP do dispositivo e outras informações de identificação são mostradas.
3. Clique no botão **Iniciar** do **Utilitário Dell DRAC** para abrir o utilitário DRAC do dispositivo ou clique no botão **Iniciar** do **Administrador de alimentação do Dell DRAC** para abrir o OpenManage Server Administrator do dispositivo em uma nova janela.

Os logs do Dell DRAC estão disponíveis no Management Suite

Três logs do utilitário OpenManage Server Administrator são mostrados no console de inventário de tempo real do Management Suite.

- **Log Dell DRAC:** controla todos os eventos registrados pelo Administrador do servidor como, por exemplo, atividade de login, status da sessão, status da atualização do firmware e interação entre o DRAC e outros componentes do dispositivo. As informações mostradas no Management Suite incluem gravidade do evento, descrição e ações de correções sugeridas em caso de erros.
- **Log de comando do Dell DRAC:** acompanha todos os comandos emitidos pelo Administrador do servidor. Mostra quais comandos foram realizados, por quem, quando, incluindo as tentativas de log in e log out e os erros de acesso.
- **Log de traço Dell DRAC:** útil para traçar detalhes sobre os eventos de comunicação da rede como, por exemplo, alerta, mensagem de pager ou conexões de rede do DRAC.

Para ver os logs de um dispositivo Dell DRAC

1. Na tela de exibição de rede do Management Suite, clique com o botão direito no dispositivo Dell DRAC e selecione **Inventário e monitoramento em tempo real**.
2. No console de inventário de tempo real, expanda **Logs**.
3. Clique em **Log Dell DRAC**, **Log de comando Dell DRAC** ou **Log de traço Dell DRAC**.

Gerenciamento de nomes de usuários para os dispositivos habilitados com o Dell DRAC

Para acessar a interface do OpenManage Server Administrator você faz o login com um nome de usuário e senha definidos para o dispositivo. O usuário padrão **root** (raiz) é o primeiro usuário na lista e não pode ser excluído, mas sua senha pode ser mudada. Podem ser adicionados até 15 usuários. Embora os nomes de usuários DRAC possam ter níveis diferentes de acesso, o Management Suite só define nomes de usuários no mesmo nível de administração.

Para acrescentar ou editar nomes de usuários e senhas para um dispositivo habilitado com o DRAC

1. Na tela de exibição de rede do Management Suite, clique com o botão direito no dispositivo Dell DRAC e selecione **Inventário e monitoramento em tempo real**.
2. No console de inventário de tempo real, clique em **Configuração do hardware**.
3. No console de configuração de hardware, expanda a **Configuração Dell DRAC** e clique em **Usuários Dell DRAC**. Aparece uma lista dos usuários definidos atuais.
4. Para mudar a senha de um usuário, clique no número do usuário e clique em **Mudar senha**. Digite e confirme a nova senha, em seguida clique em **Aplicar**. (Para designar a mesma senha para vários usuários, selecione-os usando Ctrl +clique ou Shift+clique.)
5. Para acrescentar um usuário, clique em **Adicionar usuário**. Digite um nome de usuário e senha e confirme a senha, em seguida clique em **Aplicar**. O usuário é acrescentado à lista.

   Se você digitar um nome de usuário que já constar na lista, a nova senha especificada sobregravará a existente para aquele dado nome; não será acrescentado um segundo usuário com aquele nome à lista.

6. Para excluir um usuário, clique no número do usuário e clique em **Excluir usuário**, em seguida clique em **OK**. (Para excluir vários usuários, selecione-os usando Ctrl +clique ou Shift+clique.)

Todos os usuários nessa lista têm acesso de nível de administração ao OpenManage Server Administrator.

Suporte a IPMI

O LANDesk Management Suite oferece suporte para IPMI (Intelligent Platform Management Interface) 1.5 e 2.0. IPMI é uma especificação desenvolvida pela Intel, Hewlett-Packard, NEC e Dell para definir a mensagem e a interface do sistema para hardwares habilitados para gerenciamento. O IPMI contém recursos de monitoramento e recuperação que lhe permitem acessar esses recursos independentemente do dispositivo estar ligado ou não, ou do estado do SO. Para obter mais detalhes sobre o IPMI, visite o site da web da Intel.

A monitoração IPMI é feita pelo BMC (controlador de gerenciamento de baseboard). O BMC opera com energia de espera e faz polling autônomo do status da condição do sistema. Se o BMC detectar que um elemento está com funcionamento anormal ou inativo (fora de banda), você pode configurar as ações resultantes da IPMI, por exemplo, registro de eventos, geração de alertas ou realizar ações de recuperação automática como o desligamento ou reinicialização do sistema.

É necessário ter o SMBIOS 2.3.1 ou mais recente instalado para o BMC ser detectado no sistema. Se o BMC não é detectado, podem não aparecer algumas informações que a IPMI reporta, exporta, etc.

A IPMI identifica as interfaces comuns do hardware usado para monitorar as características da condição física como temperatura, voltagem, ventiladores, fontes de alimentação e intrusão no chassi. Além da monitoramento da condição, a IPMI contém outros recursos de gerenciamento do sistema como alertas automáticos, desativação e reativação automáticas do sistema, recursos de reinicialização e controle de energia remotos e controle de recursos.

As escolhas de menu do Management Suite variam ligeiramente para um dispositivo habilitado para IPMI, dependendo do estado do sistema operacional.

Recursos de gerenciamento para os dispositivos habilitados para IPMI

Os recursos de monitoramento dependem do que foi instalado no dispositivo sendo monitorado. Qualquer dispositivo habilitado para IPMI com BMC (baseboard management controller) pode ser monitorado pelo console do administrador de maneiras limitadas sem a necessidade de agentes de gerenciamento adicionais, após o BMC ter sido configurado. Isso inclui gerenciamento fora de banda quando o dispositivo está desligado ou o SO não funciona.

O gerenciamento completo se torna disponível quando o agente de gerenciamento é instalado, um BMC está presente, o dispositivo está ligado e o SO funciona. A tabela abaixo compara a funcionalidade disponível com essas diferentes configurações.

	Apenas BMC*	BMC + agente	Agente (sem IPMI)
Gerenciamento fora da banda habilitado	X	X	
Gerenciamento dentro da banda habilitado		X	X
Dispositivo pode ser descoberto**	X	X	X
Leitura dos sensores de ambiente	X	X	Depend-ente de hardware
Alimentação ligada/desligada remotamente	X	X	X

	Apenas BMC*	BMC + agente	Agente (sem IPMI)
Leitura e limpeza do log de eventos	X	X	
Configuração de alertas	X	X	X
Leitura de informações do SO		X	X
Desativação suave		X	X
Leitura das informações do SMBIOS (processador, slots, memória)		X	X
Sincronização de IP (SO para BMC)		X	
Temporizador de vigia		X	
BMC se comunica com o servidor núcleo	X	X	
Componentes locais do Management Suite comunicam-se com o servidor núcleo		X	X
Uma gama completa de recursos de gerenciamento do Management Suite		X	

*Standard BMC. O mini BMC é uma versão reduzida de um controlador de gerenciamento de placa básica. Ele contém as funcionalidades acima descritas com as seguintes limitações:

- Não suporta serial por LAN (redireção SOL)
- Só tem um nome de usuário para gerenciamento BMC
- Utiliza apenas um canal para comunicar-se com BMC
- Tem um menor repositório de registro de eventos (SEL) de sistema

**Se o BMC não estiver configurado, ele não responderá aos pings ASF que são usados pelo produto para descobrir o IPMI. Isso significa que você terá que descobri-lo como um computador normal. Quando distribuir um agente de gerenciamento, o executável da configuração do servidor analisará o sistema e detectará que é IPMI e configurará o BMC.

Conflitos com drivers IPMI

Ao instalar este produto em um dispositivo IPMI, se esse dispositivo já tiver um driver de hardware específico IPMI instalado e esse driver for suportado por este produto, o driver será utilizado.

Se não houver driver IPMI no dispositivo, o Management Suite instalará o driver OSA IPMI.

Se tiver instalado outro software de gerenciamento que inclua dispositivos ou drivers IPMI nos dispositivos que quiser gerenciar com o este produto, você precisará desinstalar tais produtos antes de distribuir os agentes Management Suite com recursos de gerenciamento IPMI.

Por exemplo, o Microsoft Windows Server 2003 inclui suporte IPMI na instalação do WinRM (Windows Remote Management), que inclui um provedor WMI (Windows Management Instrumentation) e um driver IPMI. O Management Suite, porém, não suporta a instalação daquele driver IPMI e instala o seu próprio driver IPMI. Se o WinRM foi instalado em um dispositivos que você quer gerenciar com o Management Suite, primeiro você deve desinstalar o WinRM em Adicionar/ Remover programas do Windows.

Configuração BMC de IPMI

Use a página **Configuração IPMI BMC** para personalizar os parâmetros para comunicação com dispositivos habilitados com IPMI. Os recursos descritos abaixo estão disponíveis para dispositivos em banda. Se um dispositivo estiver fora de banda, apenas a configuração de energia e os parâmetros de usuário de BMC estarão disponíveis.

CUIDADO: É recomendado enfaticamente não mudar os parâmetros de IPMI a menos que você esteja familiarizado com a especificação IPMI e tenha uma compreensão das tecnologias utilizadas com esses parâmetros. O uso incorreto dessas opções de configuração pode impedir o Management Suite de comunicar-se com os dispositivos habilitados com IPMI.

As seguintes opções de configuração estão disponíveis:

- "Mudanças dos parâmetros de temporizador de vigia" na página 827
- "Mudança dos parâmetros de configurações de energia" na página 828
- "Parâmetros do usuário do BMC" na página 828
- "Modificação da senha do BMC" na página 829
- "Mudança das configurações de LAN" na página 829
- "Mudança da SOL (configurações Serial Over LAN)" na página 831
- "Mudança das configurações IMM" na página 831

Mudanças dos parâmetros de temporizador de vigia

O IPMI fornece uma interface para o temporizador de vigia do BMC. Esse temporizador pode ser definido com limites periódicos e é configurado para iniciar determinadas ações quando vencerem os limites (por exemplo, desligar e ligar a alimentação). O Management Suite é configurado para redefinir o temporizador periodicamente de forma que o limite não vença. Se o dispositivo tornar-se indisponível (por exemplo, for desativado ou travar), o temporizador não será redefinido e o limite vencerá iniciando, assim, a ação.

Você pode especificar o tempo limite do temporizador e selecionar uma ação para ser executada se o limite não vencer. Você pode escolher não fazer nada, fazer uma reinicialização manual (desligar e reiniciar o dispositivo), desativar o dispositivo ou executar uma ciclagem de alimentação (desativar e, em seguida, reiniciar novamente).

Você também pode definir o BMC para parar as mensagens de multidifusão ARP (Address Resolution Protocol) enquanto o temporizador de vigia estiver ativado, o que reduzirá o tráfego da rede sendo gerado. Se você suspender os ARPs, eles continuarão automaticamente se o temporizador de vigia vencer.

Para mudar os parâmetros de temporizador de vigia

1. Na tela de rede do Management Suite, clique com o botão direito no dispositivo IPMI e selecione **Inventário e monitoramento em tempo real**.
2. No painel esquerdo de navegação do console de inventário em tempo real, clique em **Configurações de hardware**.
3. Expanda a **Configuração IPMI BMC** e clique em **Temporizador de vigia**.
4. Selecione **Ativar o temporizador de vigia** para ativar o temporizador.
5. Especifique a freqüência de consulta ao temporizador (número de minutos ou segundos).
6. Selecione uma ação a ser iniciada quando o limite estabelecido do temporizador de vigia vencer.
7. Se quiser que a BMC pare de emitir mensagens ARP quando o temporizador de vigia estiver ativado, selecione **Suspender ARPs de BMC.**
8. Clique em **Aplicar**.
9. Se tiver mudado os parâmetros de temporizador de vigia, você pode reverter para os parâmetros padrão clicando em **Restaurar padrões**.

Mudança dos parâmetros de configurações de energia

Quando há queda de energia em um computador habilitado com IPMI, é possível especificar a ação esperada quando a energia for restaurada. Recomenda-se restaurar o computador a qualquer que for o estado no momento em que houve queda da energia, mas você também pode optar por mantê-lo desligado ou ligá-lo.

Para mudar os parâmetros de configurações de energia

1. Na tela de exibição de rede do Management Suite, clique com o botão direito no dispositivo IPMI e selecione **Inventário e monitoramento em tempo real**.
2. No painel esquerdo de navegação do console de inventário em tempo real, clique em **Configurações de hardware**.
3. Expanda a **Configuração IPMI BMC** e clique em **Configuração de energia**.
4. Selecione uma opção para quando a energia for restaurada.
5. Clique em **Aplicar**.
6. Se tiver mudado os parâmetros de alimentação, você pode reverter para os parâmetros padrão clicando em **Restaurar padrões**.

Parâmetros do usuário do BMC

O Management Suite autentica-se no BMC com uma combinação de nome de usuário/senha exclusiva ao BMC (separada de qualquer outro nome de usuário do Management Suite). O Management Suite reserva o primeiro nome de usuário para poder comunicar-se sempre com o BMC. Se o BMC permitir a definição de outros nomes de usuário, eles podem ser definidos com senhas para autenticação no BMC.

Você pode também especificar níveis de privilégio para cada usuário. Para IMMs avançados, você pode especificar níveis de protocolo de privilégio (telnet, http e https) para cada canal.

CUIDADO: Use de extremo cuidado ao modificar os parâmetros. Parâmetros incorretos podem desabilitar a comunicação BMC dos dispositivos com este produto.

Para mudar os parâmetros do usuário do BMC

1. Na tela de exibição de rede do Management Suite, clique com o botão direito no dispositivo IPMI e selecione **Inventário e monitoramento em tempo real**.
2. No painel esquerdo de navegação do console de inventário em tempo real, clique em **Configurações de hardware**.
3. Expanda a **Configuração IPMI BMC** e clique em **Configurações do usuário**.
4. Para limpar os dados de um nome de usuário, clique no número do índice e clique em **Limpar**.
5. Para adicionar ou mudar um nome de usuário, clique no número do índice e clique em **Editar**. Digite um nome de usuário.
7. Para definir uma senha, selecine a caixa de seleção **Definir senha**, em seguida, digite a senha e confirme-a.
8. Selecione os níveis de privilégio para a rede local e para o acesso serial.
9. Clique em **Salvar as alterações**.

Modificação da senha do BMC

O Management Suite autentica-se a um BMC de dispositivo usando o nome de usuário padrão (usuário 1 e senha). Não é possível mudar o nome do usuário, mas é possível mudar a sua senha. Quando você mudar essa definição de senha, a mudança é salva no banco de dados e no BMC.

Para mudar a senha padrão do BMC

1. Na tela de exibição de rede do Management Suite, clique com o botão direito no dispositivo IPMI e selecione **Inventário e monitoramento em tempo real**.
2. No painel esquerdo de navegação do console de inventário em tempo real, clique em **Configurações de hardware**.
3. Expanda a **Configuração IPMI BMC** e clique em **Senha**.
4. Digite a nova senha e confirme-a.
5. Clique em **Aplicar**.

Mudança das configurações de LAN

As mensagens de IPMI podem ser transmitidas diretamente do BMC através de uma interface LAN, além da interface do sistema do dispositivo. A habilitação da comunicação por LAN permite ao servidor núcleo receber alertas específicos de IPMI se o dispositivo estiver desativado. O servidor núcleo mantém essa comunicação enquanto o dispositivo tiver uma conexão física com a rede com endereço de rede válido e enquanto a alimentação principal do dispositivo permanecer conectada.

CUIDADO: Se escolher a configuração personalizada para a comunicação via rede local ou serial com o BMC, seja extremamente cuidadoso ao modificar os parâmetros. Parâmetros incorretos podem desabilitar a comunicação BMC dos dispositivos com este produto.

Se um canal de LAN estiver definido, você pode usar as configurações padrão para o BMC do dispositivo, ou mudar o endereço IP e configurações do gateway. Use essas opções para definir destinos às interceptações SNMP enviadas pelo BMC a cada evento PET (Platform Event Trap).

Também é possível mudar as configurações da string da comunidade SNMP para enviar alertas com a LAN. Ao configurar esses parâmetros, é necessário especificar a string da comunidade SNMP usada para a autenticação SNMP. Para cada configuração, é possível editar o destino da interceptação para especificar onde e como as interceptações são enviadas e se são reconhecidas.

Para definir as propriedades de configuração do canal LAN

1. Na tela de exibição de rede do Management Suite, clique com o botão direito no dispositivo IPMI e selecione **Inventário e monitoramento em tempo real**.
2. No painel esquerdo de navegação do console de inventário em tempo real, clique em **Configurações de hardware**.
3. Expanda a **Configuração IPMI BMC** e clique em **Configuração LAN**.
4. Selecione **Sempre disponível** na lista suspensa de comunicações LAN para manter aberto o acesso ao BMC. Se você selecionar **Desativado**, não terá acesso LAN ao BMC quando o dispositivo estiver fora de banda.
5. Selecione o **Nível de privilégio de usuário** para o canal: O **Nível Administrador** tem acesso a todos os comandos, enquanto o **Nível Usuário** é limitado ao acesso somente-leitura. Você terá um conjunto de recursos limitados se selecionar Nível Usuário.
6. Selecione **Desativar permanentemente os ARPs do BMC** para desativar as mensagens ARP do BMC. Isso reduz o tráfego na rede mas pode impedir a comunicação com o BMC quando o dispositivo estiver fora de banda.
7. Selecione **Desativar as respostas do ARP** para que o BMC pare de enviar respostas de mensagens ARP quando o SO não estiver disponível. Se você ativar essa configuração, poderá impedir a comunicação com o BMC quando o dispositivo estiver fora de banda.
8. As configurações IP para o canal LAN são definidas automaticamente se o BMC estiver sincronizado com o canal do SO. Se não estiver, a caixa de seleção sob a guia **Configurações IP** estará selecionada. A caixa pode permanecer selecionada para usar as configurações DHCP fornecidas automaticamente ou desmarque a caixa e edite os campos de texto com configurações estáticas. São preferíveis as configurações automáticas.
9. Clique na guia **Enviar alertas através da rede local** para definir as configurações de string de comunidade SNMP (veja os detalhes a seguir).
10. Clique em **Aplicar** para salvar as mudanças.

NOTA: Se você clicar no botão **Restaurar padrões** nesta página, as configurações sob o cabeçalho **Propriedades do canal LAN** serão redefinidas para os valores padrão, mas as outras configurações na página não serão mudadas. Se você mudar qualquer dado na guia **Configurações de IP** e clicar em **Aplicar**, será necessário redefinir manualmente essas configurações.

Para mudar as propriedades da opção Enviar alertas com a LAN

1. Abra a **Configuração LAN** página (etapas de 1 a 3, acima).
2. Clique na guia **Enviar alertas com a LAN**.
3. Selecione a caixa de seleção **Ativado** para ativar o envio de alertas SNMP.
4. Especifique a **String de comunidade SNMP** para ser usada com a autenticação SNMP.

5. Para configurar os destinos da interceptação, clique duas vezes no número do índice para abrir a caixa de diálogo **Propriedades**.
6. Selecione **Ativar este destino de alerta**. Especifique o endereço IP ao qual os alertas serão enviados pelo BMC, assim como o endereço MAC correspondente.
7. Especifique o número de vezes para as tentativas, a freqüência de tentativas e o gateway preferencial a ser usado.
8. Se você quiser que os alertas sejam reconhecidos (o que aumenta o tráfego gerado na rede), selecione a caixa de seleção **Reconhecimento de alertas**.
9. Clique em **OK**.
10. Na página de configuração da LAN, clique em **Aplicar** quando todos os parâmetros estiverem completos.

Mudança da SOL (configurações Serial Over LAN)

Use as opções de configuração SOL (Serial Over LAN) para personalizar os parâmetros de modem serial em utilizações especiais, como, por exemplo, redirecionar mensagens POST do BIOS à porta serial. Se o BMC for necessário para discar uma conexão de modem, serão também necessários parâmetros específicos de modem como, por exemplo, strings de inicialização e strings de discagem.

Para a operação com modem serial, pode ser necessário configurar o BIOS e as configurações de jumper. Consulte a documentação para ver os detalhes sobre o dispositivo específico.

CUIDADO: Se você escolher a configuração personalizada para a comunicação via rede local ou serial com o BMC, seja extremamente cuidadoso ao modificar os parâmetros. Parâmetros incorretos podem desabilitar a comunicação BMC dos dispositivos com este produto.

Para mudar os parâmetros de configurações do SOL

1. Na tela de exibição de rede do Management Suite, clique com o botão direito no dispositivo IPMI e selecione **Inventário e monitoramento em tempo real**.
2. No painel esquerdo de navegação do console de inventário em tempo real, clique em **Configurações de hardware**.
3. Expanda a **Configuração IPMI BMC** e clique em **Configuração do SOL**.
4. Selecione **Ativar comunicações SOL** para ativar o SOL.
5. Selecione o mínimo **Nível de usuário requerido para ativar o SOL**.
6. Selecione **Taxa de transmissão para as sessões SOL** apropriadas para a configuração de hardware do dispositivo.
7. Clique em **Aplicar**.

Mudança das configurações IMM

A página **Configuração IMM** só é mostrada para os dispositivos IPMI equipados com uma placa integrada IMM avançada. As opções nesta página permitem ativar ou desativar os protocolos e recursos para uso com o dispositivo habilitado para o IMM. Consulte a documentação do fabricante do IMM antes de efetuar quaisquer mudanças a essas configurações.

Para mudar os parâmetros de configurações do IMM

1. Na tela de exibição de rede do Management Suite, clique com o botão direito no dispositivo IPMI e selecione **Inventário e monitoramento em tempo real**.
2. No painel esquerdo de navegação do console de inventário em tempo real, clique em **Configurações de hardware**.
3. Expanda a **Configuração IPMI BMC** e clique em **Configuração IMM**.
4. Marque as caixas de seleção nos protocolos e recursos que quiser ativar e acrescente as definições necessárias.

   Opções disponíveis incluem KVM, SNMP, telnet, alerta SMTP, HTTP e HTTPS.

5. Clique em **Aplicar**.

Intel vPro

Configuração de dispositivos Intel vPro

Os dispositivos equipados com a funcionalidade Intel vPro devem ser configurados (ou "provisionados") ao serem instalados e ligados pela primeira vez para habilitar os recursos vPro. Este processo inclui várias medidas de segurança para assegurar que somente os usuários autorizados tenham acesso aos recursos de gerenciamento da Intel vPro.

Os dispositivos Intel vPro comunicam-se com um servidor de provisionamento na rede. Esse servidor de provisionamento detecta as mensagens dos dispositivos Intel vPro na rede e permite à equipe de TI gerenciar os servidores através de comunicação fora de banda, independente do estado do SO dos dispositivos. O servidor núcleo age como um servidor de provisionamento para os dispositivos Intel AMT e inclui recursos para adjudá-lo a configurá-lo. Você poderá então gerenciar os dispositivos com ou sem agentes de gerenciamento do adicionais.

Opções de provisionamento do Intel vPro

Há três maneiras gerais que você pode provisionar dispositivos Intel vPro. O método de Provisionamento que você usa depende do número da versão do Intel AMT dos dispositivos que você gerencia e das suas próprias preferências. Informações sobre cada método de provisionamento é fornecido em outros tópicos de ajuda como observado abaixo.

Provisionamento de um toque (usando IDs de provisionamento)

Com o Provisionamento de um toque você pode usar Management Suite para gerar um conjunto de IDs de provisionamento (PID e PPS). Esses IDs são inseridos no BIOS do dispositivo para garantir uma conexão segura com o servidor de provisionamento durante o processo inicial de provisionamento. Este processo de um toque pode ser usado para configurar dispositivos com a versão 2.0 e mais recente.

Para mais informações, consulte "Uso de IDs de provisionamento (provisionamento de um toque)" na página 836.

O provisionamento de sem toque (configuração remota usando certificados)

Dispositivos com release 2.2/2.6 e mais recente podem também ser configurados usando a configuração remota (também conhecida como provisionamento sem toque). Este processo não exige a transferência de IDs PID/PPS, mas é iniciada automaticamente depois do pacote "hello" dos dispositivos ser recebido pelo servidor de provisionamento (servidor núcleo) ou depois de um agente de gerenciamento LANDesk ser distribuído em um dispositivo Intel vPro. Um certificado de instalação cliente Intel de um fornecedor autorizado de certificação deve ser instalado no servidor núcleo para usar a configuração remota.

Para dispositivos com Intel vPro versão 3.0 e mais recente, uma configuração "bare metal" ou remota sem agente é também suportada.

Para mais informações, consulte "Uso do provisionamento remoto (provisionamento sem toque)" na página 842

Provisionamento automático para o Intel vPro 6.2 e acima

O Management Suite provisiona automaticamente dispositivos Intel vPro com versão AMT 6.2 e acima. Se você inserir uma senha na caixa de diálogo da Configuração geral do Intel vPro, mas não tiver definido uma uma PID nos dispositivos ou forneceu um certificado sem toque, seus dispositivos são provisionados usando o modo de Controle de cliente. Este modo limita algumas das funcionalidades do Intel vPro, refletindo o baixo de nível de confiança necessário para concluir a configuração do dispositivo.

Se você inserir uma senha na caixa de diálogo da Configuração geral do Intel vPro, e tiver definido uma uma PID nos dispositivos ou forneceu um certificado sem toque, seus dispositivos são provisionados usando o modo de Controle de Admin, que não limita as funcionalidades do Intel vPro, refletindo um maior nível de confiança associado a configuração do dispositivo.

Para mais informações, consulte "Provisionamento baseado em host" na página 844.

NOTA: Observe que as informações nesta seção são uma descrição geral do processo de configuração Intel vPro. Contudo, fabricantes individuais implementam a funcionalidade Intel vPro de diferentes maneiras e deve haver diferenças em tais áreas, como acesso a Intel AMT ou à tela ME BIOS, redefinição do dispositivo ao modo de fábrica (não configurado) ou de modo que pares chave PID/PPS sejam fornecidos. Consulte a documentação e as informações de suporte fornecidas pelos fabricantes do dispositivo antes de iniciar o processo de configuração.

Uso de endereços IP estáticos com os dispositivos Intel vPro

Como os dispositivos Intel vPro possuem dois componentes com endereços IP atribuídos – o chip Intel vPro e o sistema operacional do dispositivo – é possível haver duas entradas na sua lista de dispositivos descobertos para o mesmo dispositivo Intel vPro. Isso só acontecerá se você preferir usar um endereço IP estático em vez do DHCP.

Para usar endereços IP estáticos com dispositivos Intel vPro, o firmware Intel vPro deve ser configurado com o próprio endereço MAC. (Entre em contato com a Intel para obter instruções sobre como reinstalar o firmware e configurá-lo corretamente.)

Uma vez configurado, o dispositivo Intel vPro terá endereço MAC, endereço IP e nome de host diferentes daqueles do sistema operacional do dispositivo. Para que seja possível gerenciar dispositivos Intel vPro corretamente, é necessário usar as seguintes configurações para DHCP e endereços IP estáticos:

- **DHCP**: o sistema operacional e a Intel vPro usam DHCP e os nomes de host são os mesmos.
- **IP estático**: o sistema operacional e a Intel vPro estão configurados para usar endereços estáticos e eles são diferentes. Os endereços MAC e os nomes de host também são diferentes.

Se um computador Intel vPro 2.x for provisionado no modo Enterprise, o único meio de comunicação será através do envio do pacote de "alô" ao servidor de instalação e configuração. Depois que o computador for gerenciado pelo software da LANDesk, as operações do Intel vPro poderão ser executadas nele normalmente. Você não deve descobrir e gerenciar o endereço IP do sistema operacional. Caso contrário haverá duas entradas de computador representando o mesmo equipamento. Como o único identificador comum entre os dois dispositivos é o GUID AMT, e como ele não é encontrado remotamente pelo dispositivo do sistema operacional, as duas entradas não podem ser mescladas.

Se desejar instalar os agentes do LANDesk, você não poderá instalar os agentes por envio porque o único endereço IP no banco de dados é o endereço IP Intel vPro, mas o utilitário de instalação por envio necessita acessar o sistema operacional. Em vez disso, os agentes devem ser puxados (do dispositivo administrado Intel vPro) mapeando uma unidade de compartilhamento do local onde você salvou um pacote de instalação de cliente independente e executando o arquivo executável da configuração de agente.

Antes de puxar os agentes, recomendamos que você mude uma configuração no utilitário de Serviços de configurações que força o servidor núcleo a verificar o AMT GUID como parte de dispositivo identificador.

Para usar o AMT GUID como um atributo de identidade

1. Clique em **Iniciar > Todos os programas > LANDesk > Configuração de serviços LANDesk**.
2. Na guia **Inventário** , clique em **IDs de dispositivo** para gerenciar os registros duplicados.
3. Na **Lista de atributos**, expanda **Informações da AMT**.
4. Role para baixo e mude o atributo **AMT GUID** para a lista **Atributos de indentidade**.

   Isso forçará o GUID AMT a ser um dos atributos que podem identificar unicamente um computador.

Após a mudança dessa configuração (quando a análise de inventário do dispositivo gerenciado Intel vPro for importada no banco de dados), o serviço de Inventário irá comparar o GUID AMT do dispositivo que já está no banco de dados com as informações do sistema operacional no arquivo de análise.

Mudança da senha nos dispositivos com Intel vPro

Uma senha segura é necessária para se comunicar e provisionar os novos dispositivos Intel vPro. Para os dispositivos que você gerenciará, a senha digitada na Tela de configuração da Intel AMT (acessada no BIOS do dispositivo) deve ser a mesma digitada na caixa de diálogo Configuração geral do Intel vPro. A senha é salva no banco de dados e aplicada globalmente para provisionamento de dispositivos com Intel vPro.

O Intel vPro exige o uso de uma senha forte para ativar comunicações seguras. As senhas devem satisfazer aos seguintes requisitos:

- Ter pelo menos 8 caracteres
- Incluir pelo menos um número (de 0 a 9)
- Incluir pelo menos um caractere ASCII não alfanumérico (por exemplo !, &, %)
- Conter caracteres latinos maiúsculos e minúsculos ou caracteres não ASCII (UTF+00800 e acima)

Após a configuração, é necessário mudar as senhas regularmente, como parte da manutenção da TI. Você pode usar uma senha diferente para cada dispositivo Intel vPro ou aplicar uma nova senha a múltiplos dispositivos. As novas senhas que você inserir são armazenadas no banco de dados e usadas pelo Management Suite para comunicar-se com segurança com os dispositivos gerenciados Intel vPro.

Provisionamento baseado em host para o Intel vPro 6.2 e acima

O Management Suite usa o provisionamento baseado em host para dispositivos com a versão 6.2 do AMT e acima. Se você inserir uma senha na caixa de diálogo da Configuração geral do Intel vPro, mas não tiver definido uma uma PID nos dispositivos ou forneceu um certificado sem toque, seus dispositivos são provisionados usando o modo de Controle de cliente. Este modo limita algumas das funcionalidades do Intel vPro, refletindo o baixo de nível de confiança necessário para concluir a configuração do dispositivo.

Se você inserir uma senha na caixa de diálogo da Configuração geral do Intel vPro, e tiver definido uma uma PID nos dispositivos ou forneceu um certificado sem toque, seus dispositivos são provisionados usando o modo de Controle de Admin, que não limita as funcionalidades do Intel vPro, refletindo um maior nível de confiança associado a configuração do dispositivo.

Mudar a senha do Intel vPro

Para mudar a senha em todos os dispositivos com Intel VPro

1. No servidor núcleo, clique em **Configurar > Opções do Intel vPro > Configuração geral**.
2. Em **Instalação e configuração** digite uma senha forte e confirme-a.
3. Para aplicar a senha a todos os dispositivos Intel vPro gerenciados no momento, selecione a caixa de seleção **Sincronizar esta senha**.
4. Se você tem um ambiente de configuração altamente seguro e prefere não usar o modo TLS para configurar novos dispositivos, marque a caixa de seleção **Usar comunicações não-TLS**. Esta opção não é recomendada por causa dos riscos de segurança do uso de um método de comunicação menos seguro.
5. Clique em **OK**.

Essa mudança será feita quando a configuração do cliente for executada.

Para mudar a senha em um dispositivo com Intel VPro

1. Na lista **Todos os dispositivos**, clique com o botão direito em um dispositivo gerenciado Intel vPro e selecione **Alterar senha do Intel vPro**.
2. Digite e confirme a nova senha.
3. Clique em **OK**.

Uso de IDs de provisionamento (provisionamento de um toque)

Os dispositivos Intel vPro comunicam-se com um servidor de provisionamento na rede. Esse servidor de provisionamento detecta as mensagens dos dispositivos Intel AMT na rede e permite à equipe de TI gerenciar os servidores através de comunicação fora da banda, independente do estado do SO dos dispositivos. O servidor núcleo age como um servidor de provisionamento para os dispositivos Intel AMT e inclui recursos para adjudá-lo a configurá-lo.

Gere um ID de provisionamento (PID) e uma Senha de provisionamento (PPS) para cada dispositivo Intel vPro que quiser provisionar. Um PID é um ID criptografado de oito caracteres usados para assegurar que o usuário tenha as credenciais necessárias para configurar um dispositivo Intel vPro. PPS é uma senha de 32 caracteres para autenticar o PID. O PID e a PPS são comparados entre si.

Processo de uso do Provisionamento de IDs do Intel vPro

Esta seção descreve o processo de usar provisionamento de um toque para o Intel vPro 2.0 e mais recente.

Quando um dispositivo Intel vPro é recebido, o técnico de TI monta o computador e o ativa. Após ativar o dispositivo, o técnico faz a conexão à Tela de configuração Intel ME (Management Engine) baseada em BIOS e muda a senha padrão (admin) para uma senha forte. Isso permite o acesso à Tela de configuração da Intel AMT.

Na Tela de configuração da Intel AMT, as seguintes informações de pré-provisionamento são inseridas:

- Um ID de provisionamento (PID)
- Uma PPS (do inglês, pre-provisioning passkey / chave de acesso do pré-provisionamento), também conhecida como PSK (do inglês, pre-shared key / chave pré-compartilhada)
- O endereço IP do servidor de provisionamento
- A porta 9971 como a porta para a comunicação com o servidor de provisionamento
- O modo Enterprise deve ser selecionado
- O nome de host do dispositivo Intel vPro

A PPS é compartilhada pelo servidor de provisionamento e o dispositivo gerenciado, mas não pode ser transmitida na rede por motivos de segurança. Ela precisa ser digitada manualmente no dispositivo (na Tela de configuração da Intel AMT). Pares PID/PPS são gerados pelo Management Suite e armazenados no banco de dados. Você pode imprimir uma lista de pares de ID para uso no provisionamento ou exportar os pares de ID para um arquivo-chave em uma unidade USB.

O técnico de TI deve inserir o endereço IP do servidor núcleo do Management Suite para o Servidor de provisionamento e especificar a porta 9971. Caso contrário, por padrão, o dispositivo Intel AMT enviará uma multidifusão geral que só poderá ser recebida se o servidor de configuração estiver escutando a porta 9971.

O nome de usuário e senha padrão para o acesso à Tela de configuração da Intel AMT são "admin" e "admin". O nome do usuário permanece o mesmo mas a senha deve ser alterada durante o processo de provisionamento para uma senha forte. A nova senha é inserida no diálogo de configuração geral do Intel vPro conforme descrito nas etapas de procedimento abaixo. Após cada dispositivo ter sido configurado, você poderá alterar a senha individualmente por dispositivo, mas para fins de provisionamento, será necessário usar a senha encontradas no diálogo de configuração geral.

Após as informações acima terem sido inseridas na Tela de configuração da Intel AMT, o dispositivo enviará mensagens de “alô” quando for conectado à rede pela primeira vez ao tentar se comunicar com o servidor de provisionamento. Se esta mensagem for recebida pelo servidor de provisionamento, o processo de provisionamento será iniciado quando o servidor estabelecer uma conexão com o dispositivo gerenciado.

Quando o servidor núcleo recebe a mensagem de alô e verifica as chaves PID, ele configura o dispositivo Intel vPro no modo TLS. O modo TLS (Transport Layer Security) estabelece um canal seguro de comunicações entre o servidor núcleo e o servidor gerenciado enquanto o provisionamento é concluído. Este processo inclui a criação de um registro no banco de dados com o UUID do dispositivo e as credenciais criptografadas. Quando os dados do dispositivo estiverem no banco de dados, o dispositivo será mostrado na lista de dispositivos não gerenciados.

Quando o provisionamento de um dispositivo Intel vPro tiver sido feito pelo servidor núcleo, ele poderá ser gerenciado somente por meio da funcionalidade Intel vPro. Para fazer isso, você poderá selecioná-lo na lista de dispositivos não gerenciados e adicioná-lo aos seus dispositivos gerenciados. Você pode também distribuir os agentes de gerenciamento para o dispositivo para usar recursos adicionais de gerenciamento.

O processo recomendado para o provisionamento dos dispositivos Intel vPro é o como segue.

1. Especifique uma nova senha forte para profisionamento de dispositivos Intel vPro.
2. Gera um lote de IDs de provisionamento do Intel vPro (PID e PPS). Imprima a lista de chaves ou exporte-as para uma unidade USB.
3. Conecte-se à tela de configuração do Intel ME do dispositivo a partir do BIOS e altere a senha padrão para uma forte.

4. Conecte-se à Tela de configuração da Intel AMT. Insira um par de chaves PID/PPS da lista de IDs de provisionamento que você imprimiu. Insira o endereço IP do servidor núcleo (servidor de provisionamento) e especifique a porta 9971. Não deixe de selecionar o modo Enterprise para o provisionamento. Insira o nome host do dispositivo Intel vPro.
5. Saia da tela do BIOS. O dispositivo começará a enviar mensagens de "alô".
6. O servidor núcleo recebe uma mensagem de "alô" e verifica se o PID está na lista de chaves geradas. Se houver uma correspondência, o dispositivo será provisionado.
7. O dispositivo é adicionado à lista de descoberta de dispositivos não gerenciados.
8. Selecione o dispositivo e adicione-o aos seus dispositivos gerenciados (clique em **Alvo** na barra de ferramentas, clique na guia **Gerenciar** e, em seguida, clique em **Mover**). Você pode optar por gerenciá-lo como um dispositivo sem agente ou distribuir agentes de gerenciamento a ele para obter recursos de gerenciamento adicionais.

Para obter instruções detalhadas para o passo 1, veja "Mudar a senha do Intel vPro" na página 836

Para obter instruções detalhadas para o passo 2, veja "Gera um lote de IDs de provisionamento do Intel vPro" na página 838

Erros no processo de provisionamento

Se você digitar um PID e uma PPS que não formam um par correto (por exemplo, a PPS forma um par com uma PID incorreta), um erro será mostrado no registro de alerta e o provisionamento não prosseguirá para aquele dispositivo. Será necessário reiniciar o dispositivo e inserir novamente um par PID/PPS correto na Tela de configuração da Intel AMT.

Se, ao digitar um PID ou PPS, a Tela de configuração da Intel AMT mostrar um erro, você digitou o PID ou PPS incorreto. Uma soma de comprovação é feita para confirmar se o PID e o PPS estão corretos.

Gera um lote de IDs de provisionamento do Intel vPro

IMPORTANTE: Antes de gerar IDs Intel vPro, é necessário criar uma senha Intel vPro para a conta "admin" padrão e sincronizar a senha com todos os dispositivos Intel vPro gerenciados. See "Mudança da senha nos dispositivos com Intel vPro" on page 835.

1. Clique em **Configurar > Opções Intel vPro > Criação de ID**.
2. Digite o número de IDs a serem gerados (geralmente, o número de dispositivos que você planeja provisionar).
3. Se desejar usar um prefixo diferente para os PIDs, digite-o na caixa de texto **Prefixo PID**. Esse prefixo só poderá conter caracteres alfabéticos maiúsculos e números do conjunto de caracteres ASCII. O prefixo pode conter no máximo 7 caracteres.
4. Digite um nome de lote para identificar este grupo de IDs gerados.
5. Clique em **Gerar IDs**.
6. Após os IDs terem sido gerados, clique em **Imprimir lista de IDs** para imprimir a lista de IDs. (Serão impressos somente os IDs mostrados na lista atualmente.) O recurso de impressão do navegador abre automaticamente.
7. Para ver todos os IDs gerados anteriormente, selecione **Exibir todos** na lista suspensa **Ver IDs de lote**.

8. Para ver um lote de IDs gerados, selecione o nome do lote na lista suspensa **Ver IDs de lote**.
9. Para imprimir uma lista dos IDs gerados para referência futura, clique em **Imprimir lista de IDs**. A caixa de diálogo de impressão do Windows abre; selecione uma impressora e clique em **Imprimir**.

As chaves de provisionamento são armazenadas no banco de dados para referência futura, à medida que você configura novos dispositivos Intel vPro. À medida que os dispositivos forem configurados e as chaves de provisionamento forem utilizadas, a página **Gerar IDs vPro** mostrará os IDs utilizados esmaecidos para que você possa controlar quais IDs foram usados.

Notas de chaves de provisionamento

Um prefixo PID é adicionado para facilitar a identificação dos IDs como PIDs, mas o uso de prefixos não é obrigatório. Recomendamos o uso de 0 a 4 caracteres. Você pode usar o máximo de 7 caracteres para o prefixo.

Para identificar lotes de chaves de provisionamento, especifique um nome de lote. Este deve ser um nome descritivo que indique os dispositivos aplicados aos IDs. Por exemplo, você pode gerar lotes para cada organização na sua empresa e atribuir nomes como Desenvolvimento, Marketing, Finanças, etc. Se desejar ver os IDs gerados posteriormente, digite o nome do lote e clique em **Ver IDs de lote** para ver uma lista somente com esses IDs.

Clique aqui para obter descrições das opções do Intel vPro IDs

Gerar IDs

Use esta seção para digitar um critério para gerar o e PID e o PPS.

- **Números de IDs para gerar**: inserir o número de IDs que você deseja criar (normalmente o número de dispositivos você deseja provisionar). Você deve inserir um valor ou as IDs não poderão ser geradas.
- **Prefixo PID para IDs gerados**: Digite um prefixo para ajudar a identificar os PIDs. Um prefixo PID é adicionado para facilitar a identificação dos IDs como PIDs, mas o uso de prefixos não é obrigatório. Recomendamos o uso de 0 a 4 caracteres. Você pode usar o máximo de 7 caracteres para o prefixo.
- **Nome do lote de IDs gerados**: Digite um nome para identificar o lote de IDs gerados. Esse nome é opcional. Ele deve ser um nome descritivo que indique os dispositivos aplicados aos IDs. Por exemplo, você pode gerar lotes para cada organização na sua empresa e atribuir nomes como Desenvolvimento, Marketing, Finanças, etc. Se desejar ver os IDs gerados posteriormente, digite o nome do lote e clique em **Ver IDs de lote** para ver uma lista somente com esses IDs.

Ver IDs de lote

Se você digitar os nomes para lotes diferentes de IDs gerados, os nomes são mostrados na lista suspensa **Ver os IDs de lote**. Os IDs disponíveis no nome de lote selecionado são mostrados na caixa de lista abaixo da lista suspensa. Se você não gerar IDs com um nome de lote, todos os IDs são exibidos na caixa de lista.

Esses IDs são armazenados no banco de dados para referência futura à medida que você configura novos dispositivos Intel vPro. Como os dispositivos são provisionados e as chaves de provisionamento são utilizadas, a página **Gerar IDs de Intel vPro** mostra o esmaecido nos IDs que foram usados.

Importar/Exportar IDs

As IDs geradas podem ser exportadas para um arquivo chamado setup.bin. O arquivo setup.bin pode ser armazenado em um drive USB que pode ser transportado para outros servidores de provisionamento para que as IDs que ainda não foram usadas possam ser importadas e colocadas em uso com outros dispositivos Intel vPro.

Imprimir lista de ID

O recurso Imprimir lista de ID imprime os IDs atualmente mostrados na lista. Se você tiver selecionado **Mostrar todos** ou **Sem nome de lote** da lista suspensa **Ver IDs de lote**, todos os IDs disponíveis são impressos. Se você selecionar um nome de lote da lista suspensa **Ver IDs de lote**, somente os IDs nesse lote são impressos.

Importando e exportando IDs de provisionamento

Você pode gerar IDs de provisionamento e exportá-los para um arquivo de chaves para usá-los no provisionamento de dispositivos Intel vPro com uma unidade USB. Os IDs exportados são salvos em um arquivo setup.bin que pode ser copiado para uma unidade USB. Como essa unidade USB, você poderá preencher automaticamente os campos de PID/PPS no BIOS da Intel AMT à medida que provisiona novos dispositivos Intel vPro antes de descobri-los e gerenciá-los.

Se um fabricante fornecer um conjunto de IDs de provisionamento para os dispositivos Intel vPro que você adquiriu, será possível importar esses IDs no banco de dados núcleo para que o servidor núcleo reconheça tais dispositivos como Intel vPro e os descubra automaticamente.

Esses dois processos são descritos a seguir.

Exportação de IDs de provisionamento para uso com uma unidade USB

O Management Suite gera IDs de provisionamento (PID/PPS) que você usa no provisionamento de novos dispositivos Intel vPro. Você poderá imprimir uma lista dos IDs gerados e inseri-los manualmente ao fazer o provisionamento de cada dispositivo. Uma outra opção é exportar os IDs para um arquivo de chaves setup.bin, salvá-lo em uma unidade USB e usar essa unidade para prover os dispositivos. Isso pode reduzir os erros de provisionamento porque não é necessário digitar os IDs manualmente em cada dispositivo.

A unidade USB deverá estar formatada em FAT-16 para que este processo funcione.

O arquivo setup.bin é criado com um formato de arquivo de chaves específico definido pela Intel. Ao fazer o provisionamento do novo dispositivo Intel vPro, você deverá conectar a unidade USB ao dispositivo e reinicializá-lo. Durante o processo de inicialização, um par de IDs de provisionamento (PID e PPS) é obtido do arquivo setup.bin e inserido no BIOS Intel AMT do dispositivo. Quando o dispositivo enviar sua mensagem de "alo" na rede, o servidor núcleo o reconhecerá e poderá se comunicar com segurança com ele porque as IDs de provisionamento existem no banco de dados núcleo.

Para exportar um lote de IDs de provisionamento para uso com uma unidade USB

1. Clique em **Configurar > Opções do Intel vPro > Geração de ID > Importar/Exportar IDs**.
2. Selecione **Exportar IDs AMT para o arquivo setup.bin**. O número de IDs disponíveis para exportar é mostrado em parênteses próximo desta opção.

3. Insira e confirme a senha do vPro Management Engine. Esta é a senha que permite o seu acesso aos recursos de gerenciamento do Intel vPro. A senha padrão é "admin" se você já não tiver configurado uma senha para o Mecanismo de gerenciamento.
4. Digite um número na caixa de texto **Número de IDs para exportar**. Você precisa digitar pelo menos "1" nesse campo. O número máximo que você pode digitar é o número de IDs disponíveis indicado próximo da opção **Exportar IDs AMT para o arquivo setup.bin**.
5. Na caixa de texto **Especifique o local para setup.bin**, digite um caminho ou navegue para a pasta onde deseja salvar o arquivo setup.bin.

   Você poderá salvar o arquivo em qualquer local e copiá-lo para uma unidade USB ou simplesmente especificar o local da unidade USB se ela estiver conectada ao servidor núcleo. Para usar o arquivo setup.bin no provisionamento, salve-o no diretório raiz da unidade USB.
6. Clique em **OK** e em **Fechar**.

NOTA: Os IDs gerados são listados com outros IDs gerados na página **Gerar IDs de Intel vPro**. Os IDs serão sombreados na lista para indicar que eles não estão disponíveis para o provisionamento de outros dispositivos.

Para usar os IDs de provisionamento exportados em novos dispositivos Intel vPro

1. Exporte um lote de IDs de provisionamento conforme descrito acima. Em seguida, salve o arquivo setup.bin no diretório raiz de uma unidade USB.
2. Em cada novo dispositivo Intel vPro, conecte a unidade USB ao dispositivo e reinicialize-o.

Ao inicializar, o dispositivo acessa o arquivo setup.bin e obtém um par de IDs de provisionamento (PID e PPS) disponível para usá-lo no processo de provisionamento. Em seguida, o par de IDs de provisionamento é marcado como usado para que não possa ser usado por outro dispositivo. O próximo dispositivo que for provisionado usará então o próximo par de IDs disponível.

Para que este processo funcione corretamente, o nome de usuário padrão e a senha de acesso ao BIOS Intel AMT não poderão ter sido alterados (o padrão é, normalmente, admin/admin). Não poderá haver IDs de provisionamento já inseridas no dispositivo.

Importação de IDs de provisionamento de um arquivo de chaves no banco de dados núcleo

Se um fabricante fornecer um conjunto de IDs de provisionamento para os dispositivos Intel vPro que você adquiriu, será possível importar esses IDs no banco de dados núcleo para que o servidor núcleo reconheça tais dispositivos como Intel vPro e os descubra automaticamente. Os IDs são fornecidos pelo fabricante em um arquivo setup.bin quando os dispositivos são adquiridos.

Para importar os IDs no banco de dados núcleo, basta navegar para o local do arquivo setup.bin fornecido pelo fabricante (em um CD ou DVD, mas o arquivo pode ser copiado para qualquer unidade). Após esses IDs serem salvos no banco de dados, quando os dispositivos Intel vPro forem iniciados e enviarem mensagens de "alô", o servidor núcleo os reconhecerá e descobrirá os dispositivos.

Para importar IDs de provisionamento de um arquivo de chaves no banco de dados núcleo

1. Clique em **Configurar > Opções do Intel vPro > Geração de ID > Importar/Exportar IDs**.
2. Selecione **Importar de um arquivo chave USB**.

3. Na caixa de texto **Especifique o local para setup.bin**, digite um caminho ou navegue para a pasta que contém o arquivo setup.bin.
4. Clique em **OK** e em **Fechar**.

Os IDs de provisionamento são adicionados ao banco de dados núcleo e listados no diálogo **Gerar IDs vPro**.

Uso do provisionamento remoto (provisionamento sem toque)

Esta seção descreve o processo para uma configuração remota de dispositivos com Intel vPro 2.2/2.6 e mais recente.

A configuração remota permite que você configure um dispositivo em estado padrão de fábrica através do processo de configuração e adicione um perfil Intel AMT para deixá-lo pronto para o gerenciamento fora de banda. Quando o dispositivo for ligado pela primeira vez e conectado a uma rede, ele começa a enviar mensagens "alô" para o Servidor de Instalação e Configuração (ao gerenciar dispositivos com produtos LANDesk, o servidor núcleo age como o Servidor de Instalação e Configuração). Se o Servidor de Instalação e Configuração estiver em execução, ele estabelece uma conexão segura com o dispositivo Intel vPro e inicia o processo de configuração.

Quando o processo é concluído com êxito, o dispositivo é adicionado á lista de dispositivos descobertos e pode ser gerenciado pelo servidor núcleo. O gerenciamento limitado está disponível com a única funcionalidade Intel vPro, ou um agente de gerenciamento pode ser distribuído ao dispositivo para recursos completos de gerenciamento.

O provisionamento remoto possui dois requisitos:

- É necessário o DHCP na rede, com uma entrada DNS identificando o servidor núcleo como sendo o "ProvisionServer"
- Um Certificado de instalação Cliente Intel deve ser instalado no servidor núcleo para o domínio onde o servidor núcleo é instalado (as instruções são dadas abaixo para a compra e instalação de um certificado)

Provisionamento demorado

Se um dispositivo Intel vPro estiver ligado mas não receber uma resposta do Servidor de Instalação e Configuração depois de um certo período de tempo (normalmente de 6 a 12 horas, dependendo das configurações do fabricante), ele pára de enviar pacotes alô e aguarda. Nesse ponto a funcionalidade Intel vPro não está habilitada no dispositivo.

Para configurar um dispositivo neste estado, é preciso instalar o agende de gerenciamento LANDesk no dispositivo. Quando o agente determina que o dispositivo possui capacidades Intel vPro, ele ativa a funcionalidade Intel vPro no dispositivo e envia uma chamada ao serviço de web no servidor núcleo para receber um pacote "alô". O processo de provisionamento é então iniciado no servidor núcleo.

Provisionamento Bare metal

Os dispositivos Intel vPro 3.0 suportam uma abordagem bare-metal (ou sem agente) para configuração remota. Com o Servidor de Instalação e Configuração configurado corretamente, uma entrada DNS e o certificado correto instalado no servidor núcleo, o processo de configuração é concluído sem o uso de agentes.

NOTA: Se um dispositivo Intel vPro estiver ligado mas não envia mensagens "alô" conforme descrito acima, a configuração remota pode não ser ativada no dispositivo. Isso depende da ativação da configuração remota do fabricante, definindo o Modo de Gerenciabilidade para "AMT" no dispositivo. Se esse for o caso, você pode distribuir um agente de gerenciamento LANDesk para o dispositivo para ativar a funcionalidade Intel vPro e começar a o provisionamento do dispositivo conforme descrito acima em "Provisionamento demorado".

Provisionamento baseado em host para o Intel vPro 6.2 e acima

O Management Suite usa o provisionamento baseado em host para dispositivos com a versão 6.2 do AMT e acima. Se você inserir uma senha na caixa de diálogo da Configuração geral do Intel vPro, mas não tiver definido uma uma PID nos dispositivos ou forneceu um certificado sem toque, seus dispositivos são provisionados usando o modo de Controle de cliente. Este modo limita algumas das funcionalidades do Intel vPro, refletindo o baixo de nível de confiança necessário para concluir a configuração do dispositivo.

Se você inserir uma senha na caixa de diálogo da Configuração geral do Intel vPro, e tiver definido uma uma PID nos dispositivos ou forneceu um certificado sem toque, seus dispositivos são provisionados usando o modo de Controle de Admin, que não limita as funcionalidades do Intel vPro, refletindo um maior nível de confiança associado a configuração do dispositivo.

Obtenção e instalação do Certificado de Instalação de cliente Intel

Um Certificado de Instalação Cliente Intel é necessário em todo Servidor de Instalação e Configuração. O certificado deve ser adquirido de um fornecedor de certificados aprovado e deve ser de uma classe compatível. Os seguintes fornecedores são suportados para os produtos LANDesk para os seguintes dispositivos.

NOTA: Antes de adquirir um certificado, verifique na documentação ou informações de suporte do fornecedor quais certificados são suportados no seu dispositivo.

Fornecedor/Classe do certificado	Dispositivos Intel	Dispositivos Acer	Dispositivos Lenovo
Go Daddy classe 2 CA	X	X	X
VeriSign classe 3 Primary CA-G3	X	X	X
VeriSign class 3 Primary CA-G1	X	X	X
Comodo AAA CA	X	X	
Starfield classe 2 CA			X

Ao adquirir um certificado, você precisa fornecer um arquivo CSR (certificate signing request). Este arquivo é gerado para o seu produto LANDesk juntamente com um arquivo chave particular. Depois de receber os arquivos de certificado do fornecedor, a chave particular é salva em um diretório com um arquivo com uma chave pública compartilhada e o arquivo certificado do fornecedor. Este procedimento é descrito abaixo.

Para obter um Certificado de Instalação Cliente Intel

1. Selecione um fornecedor e efetue login no site dele.
2. Gere um arquivo CSR e uma chave privada: No diretório \Program Files\LANDesk\ManagementSuite\amtprov, execute AMTProvMgr2.exe com os seguintes argumentos:
   `AMTProvMgr2.exe -domainName name.domain.com -country [código de país de 2 letras] -state [nome do estado] -city [nome da cidade] -organization [nome da organização]`
   Os argumentos que você precisa fornecer podem variar dependendo do fornecedor do certificado. O nome do domínio que você especificar deve incluir um namespace. Para ver informações de ajuda sobre os argumentos e sobre este arquivo executável, execute o arquivo de um prompt de comando com o argumento -h.

   Este executável salva dois arquivos no diretório amtprov: certreq.csr (solicitação de assinatura do certificado) e corecakey.pem (um arquivo de acesso particular).
3. Abra o arquivo certreq.csr em um editor de texto e copie o conteúdo.
4. No site do fornecedor, cole o conteúdo do arquivo certreq.csr no campo fornecido e preencha o formulário do certificado.

   Depois que a solicitação do certificado for processada, o fornecedor enviará dois arquivos: um arquivo certificado raiz (um arquivo comum ou público) e um arquivo certificado para o domínio que você especificou.
5. Faça uma cópia do arquivo de certificado raiz e renomeie a cópia para `trusted_cert.pem`.
6. Faça uma cópia do arquivo de certificado do fornecedor para o seu domínio e renomeie a cópia para `corecacert.pem`.
7. Salve os dois arquivos acima, junto ao arquivo `corecakey.pem` (gerado no passo 2 acima), para uma pasta em LDMAIN\amtprov\certStore\cert_1. Você pode armazenar até oito certificados em subpastas chamadas cert_1, cert_2 e assim por diante.
8. Se você tiver consoles adicionais, copie esses três arquivos no mesmo caminho de pasta em cada console adicional.

Provisionamento baseado em host

O Management Suite usa o provisionamento baseado em host para dispositivos com a versão 6.2 do AMT e acima. Este tópico descreve como este processo funciona e como você pode mudar um dispositivo do modo Controle de cliente para modo de Controle de admin.

Processo de provisionamento

Para cada dispositivo de Intel vPro com versão de AMT 6.2 e mais alto, o Management Suite executa um provisionamento baseado em host do dispositivo quando o dispositivo é detectado e uma senha do Intel vPro é inserida na caixa de diálogo de Configuração do Intel vPro.

Você deve ter inserido uma senha para este processo de provisionamento para iniciar e driver do Intel vPro devem ser instalados no Windows do dispositivo. No entanto, há nenhuma outra tarefa necessária para este provisionamento básico acontecer.

Se você inserir uma senha na caixa de diálogo da Configuração geral do Intel vPro, mas não tiver definido uma uma PID nos dispositivos ou forneceu um certificado sem toque, seus dispositivos são provisionados usando o modo de Controle de cliente. Este modo limita algumas das funcionalidades do Intel vPro, refletindo o baixo de nível de confiança necessário para concluir a configuração do dispositivo.

Se você inserir uma senha na caixa de diálogo da Configuração geral do Intel vPro, e tiver definido uma uma PID nos dispositivos ou forneceu um certificado sem toque, seus dispositivos são provisionados usando o modo de Controle de Admin, que não limita as funcionalidades do Intel vPro, refletindo um maior nível de confiança associado a configuração do dispositivo.

NOTA: O Management Suite não verifica se um certificado de toque- zero é válido se funciona no domínio atual; simplesmente verifica a existência de um certificado. Se por qualquer razão seu certificado não é válido, então o provisionamento continuará no modo de Controle de cliente.

Se você tem qualquer dúvida quanto ao modo de controle usado para um dispositivo Intel vPro, você pode olhar o status de dispositivo Intel vPro (clique com o botão direito no dispositivo na tela de rede e selecione **Opções do Intel vPro> Status do Intel vPro)**.

Mudar do modo de Controle de cliente para o modo de Controle de Admin

Se você tem dispositivos que foram provisionados no modo de Controle de cliente e mais tarde instala um certificado de sem toque, você pode re-provisionar os dispositivos em modo de Controle de Admin.

Para re-provisionar um dispositivo Intel vPro 6.2+

1. Instale um certificado de sem toque no servidor núcleo.
2. Na tela de rede, clique com o botão direito em um dispositivo Intel vPro e selecione **(Re) Instalar e Configurar vPro**.

O Management Suite provisionará o dispositivo no modo de Controle de Admin.

As diferenças entre modo de Controle de cliente e modo de Controle de Admin

O modo de Controle de cliente limita a funcionalidade do Intel vPro que está disponível em um dispositivo administrado. Isso reflete o nível mais baixo de confiança necessária para concluir o Provisionamento do dispositivo. A seguinte lista descreve as limitações do modo de Controle de cliente.

- O recurso de defesa do sistema não está disponível.
- Redireciona ações (IDE-R e KVM) (exceto a iniciação de uma sessão de SOL) e as mudanças nas opções de inicialização (inclusive reinicialização de SOL) exige autorização do usuário . Isto ainda habilita o pessoal do suporte de TI a resolver problemas de usuários remotamente usando o Intel AMT.
- Se um usuário de Auditor for definido, a permissão do Auditor não é exigida desfazer o provisionamento.
- Outras funções são bloqueadas para prevenir que um usuário não confiável assuma o controle da plataforma.

Para obter informações mais detalhadas, recomendamos que você consulte a última *Implementação do Intel AMT e o Guia de Referência*, no site de Intel.

Uso de Opções de energia da Intel vPro

O Management Suite contém opções para ligar e desligar dispositivos Intel vPro. Essas opções podem ser usadas mesmo quando o sistema operacional do dispositivo não está respondendo, desde que o dispositivo esteja conectado à rede e possua alimentação em modo de espera.

Quando o Management Suite inicia os comandos de opção de energia, não é possível, em alguns casos, verificar se os comandos são aceitos pelo hardware que recebe o comando. Alguns dispositivos Intel vPro podem não oferecer suporte a todos os recursos de opção de energia (por exemplo, um dispositivo pode aceitar a reinicialização da IDE-R via CD, mas não de um disquete). Consulte a documentação do fabricante do hardware se uma opção de energia não estiver funcionando com um dispositivo em particular. Também é possível verificar se há atualizações de firmware ou BIOS da Intel para o dispositivo quando as opções de energia não funcionam conforme o esperado.

Para dispositivos Intel vPro, quando você emite um comando de ligar, o Management Suite envia primeiro um comando de ativação do Intel vPro. Se esse comando não funcionar ele, então, envia um comando Wake on LAN ao dispositivo.

Ligue ou desligue a alimentação do dispositivo ou reinicialize e especifique a forma como o dispositivo é reinicializado. As opções são descritas na tabela abaixo.

Opção	Descrição
Desligar	Desliga a alimentação do dispositivo
Ligar	Liga a alimentação do dispositivo.
Reinicializar	Desliga e liga a alimentação do dispositivo novamente.
Inicialização normal	Inicia o dispositivo com o uso da seqüência de inicialização que foi definida no mesmo
Inicializar de um disco rígido local	Força uma inicialização do disco rígido do dispositivo, independentemente do modo de inicialização padrão no dispositivo
Inicializar de uma unidade de CD/DVD	Força uma inicialização do CD ou DVD do dispositivo, independentemente do modo de inicialização padrão no dispositivo
Inicialização do PXE	Ao ser iniciado, o dispositivo com suporte a PXE procura um servidor de PXE na rede. Se o encontra, uma sessão de inicialização do PXE é começada no dispositivo.
Inicialização da IDE-R	Reinicializa o dispositivo com o uso da opção de redirecionamento da IDE selecionada (veja abaixo)

Opção	Descrição
Entrar na configuração do BIOS ao ligar	Quando o dispositivo é inicializado, ele permite ao usuário entrar na configuração do BIOS
Mostra a janela de redirecionamento do console	Quando o dispositivo é inicializado, ele o faz no modo Serial over LAN para exibir uma janela de redirecionamento do console.
Redirecionamento da IDE: Reinicializa do disquete	O dispositivo é inicializado da unidade de disquete especificada.
Redirecionamento da IDE: Reinicializar do CD/DVD	O dispositivo é inicializado da unidade de CD especificada.
Redirecionamento da IDE: Reinicializar de um arquivo de imagem especificado	O dispositivo é inicializado do arquivo de imagem especificado (os arquivos de imagem de disquete deverão estar no formato .img, enquanto que os arquivos de imagem de CD deverão estar no formato .iso; veja a nota abaixo).

Para usar as opções de alimentação da Intel vPro

1. Na tela de rede, clique com o botão direito em um dispositivo Intel vPro e selecione **Opções Intel vPro > Gerenciador de inicialização remota Intel vPro**.
2. Selecione um comando de alimentação
3. Se você selecionar **Reinicializar**, selecione uma opção de inicialização.
4. Caso selecione o método de inicialização de redirecionamento da IDE, especifique um disquete, uma unidade de CD ou um arquivo de imagem.
5. Se houver uma sessão IDE-R aberta e você desejar fechá-la, clique em **Fechar sessão Close IDE-R**.
6. Clique em **Enviar** para iniciar o comando de energia ou clique em **Fechar**.

Notas sobre o uso das opções de redirecionamento da IDE

Quando as opções de redirecionamento da IDE são usadas, os arquivos de imagem de disquete devem estar no formato .img e os arquivos de imagem de CD devem estar em formato .iso. Alguns BIOS podem exigir que a imagem de CD esteja localizada em um disco rígido.

Normalmente, o Intel vPro lembra das últimas configurações de IDE-R, mas o Management Suite limpa as configurações após 45 segundos. Assim, em inicializações subseqüentes ela não reiniciará o recurso IDE-R. A sessão de IDE-R em um dispositivo Intel vPro dura 6 horas ou até o console do Management Suite ser desligado. As operações de IDE-R ainda em andamento após 6 horas são terminadas.

NOTA: Em algumas situações, um processo de inicialização IDE-R pode parecer ter vencido o tempo limite no console do SOL (serial por LAN) quando o processo de inicializaão ainda estiver em processamento. Se a imagem de inicialização leva muito tempo para inicializar e enviar dados ao console do SOL, o console para de se comunicar e a conectividade do teclado é perdida. Isso ocorre quando a

mídia usada para a inicialização apresentar tempo de resposta lento e levar mais de 60 segundos para inicializar (o qual é o valor limite mais longo permitido). Se você experimentar este problema ao inicializar com um disquete ou outra mídia, nós recomendameos que você inicialize de um arquivo de imagem de inicialização (.img) em vez de uma mídia removível.

Acesso remoto em dispostivos Intel vPro

Os dispositivos Intel vPro (versões 4.0 e mais recente) podem ser gerenciado remotamente de um console LANDesk Management Suite. Quando um dispositivo Intel vPro estiver fora da rede na qual o console Management Suite está localizado, a comunicação com o servidor núcleo — através do firewall e DMZ da rede — é ativada pela funcionalidade de acesso remoto.

O acesso remoto para dispositivos Intel vPro ativa a comunicação entre um console de gerenciamento dentro de uma rede segura e os dispositivos Intel vPro localizados fora da rede. Essa comunicação é feita através de um túnel TLS que conecta o dispositivo fora da rede com um servidor (denominado Intel vPro Gateway Server [Servidor Gateway Intel vPro]) que está tipicamente localizado na DMZ da rede. As comunicações com o Intel vPro Gateway Server (Servidor Gateway Intel vPro) são então enviadas para o servidor núcleo Management Suite pelas conexões HTTP seguras utilizando certificados confiáveis raiz e de servidor.

Para que um dispositivo gerenciado use o acesso remoto, ele deve ter:

- Uma diretiva de acesso remoto aplicada em seu firmware
- um certificado raiz confiável que corresponda ao certificado de servidor núcleo usado nos produtos LANDesk
- Um certificado cliente que corresponda ao certificado de servidor núcleo usado nos produtos LANDesk

Os recursos de acesso remoto lhe permitem criar uma diretiva de acesso remoto e aplicá-la ao firmware dos dispositivos gerenciados.

Quando você tiver configurado o dispositivo e instalado o Intel vPro Gateway Server (Servidor Gateway Intel vPro), as sessões remotas do dispositivo gerenciado serão operadas num agendamento regular que você especificar (tipicamente uma vez por dia). Quando uma sessão remota é iniciada, o dispositivo é mostrada na lista Sessão aberta na caixa de diálogo Configuração de acesso remoto do Intel vPro. Além disso, o status da página do cliente em Management Suite indica que a sessão está aberta.

NOTA: Note que quando o acesso remoto estava sendo desenvolvido, ele era denominado Acesso remoto iniciado pelo cliente ou CIRA. Se você encontrar menções do CIRA, isso se refere ao Acesso remoto. O Intel vPro Gateway Server (Servidor Gateway do Intel vPro) era antigamente denominado MPS (Management Presence Server - Servidor de gerenciamento de presença), portanto podem aparecer menções do MPS relacionadas ao Servidor Gateway. Além disso, a documentação da Intel pode referir-se a Fast Call for Help (Chamada rápida para Ajuda), que é a opção de acesso remoto iniciada pelo dispositivo cliente.

Configurando um servidor Intel vPro gateway

Você pode habilitar o acesso remoto usando um servidor na sua rede para agir como um Servidor gateway Intel. Isso requer a execução das seguintes tarefas gerais:

- Utilizar um executável de instalação em um servidor e configurá-lo para uso como um Servidor Gateway Intel vPro

- Configurar o Parâmetro de acesso remoto e as opções de Deteção de ambiente de rede no servidor núcleo Management Suite

A documentação para a configuração de acesso remoto está localizada no seu servidor núcleo, na pasta \Programs Files\LANDesk\Management Suite\Install\vpro\remoteaccess. (Esta é a pasta onde está localizado o arquivo executável.)

Configuração do acesso remoto KVM para dispositivos com Intel vPro

Os dispositivos Intel vPro (AMT versão 6 ou superior) pode ser gerenciado remotamente via KVM. Isto permite que um administrador de TI veja a tela inteira do dispositivo do cliente com controle total do teclado, do mouse e controle de vídeo do dispositivo.

A função de KVM é compatível com dois modos de conexão: direto e entrada (conhecido como MPS). Ele também é compatível com dois tipos de comunicação: TLS (padrão) e não-TLS. Quando um dispositivo AMT é provisionado, a função KVM é desativada por padrão. A função KVM é restrita a uma licença núcleo ou console. Um usuário independente do controle remoto não pode usar função KVM.

Para configurar parâmetros KVM

1. Clique em **Configurar > Opções do Intel vPro > Configurações da KVM.**
2. Na caixa de diálogo de **ativação da KVM,** clique em **Ativar função KVM** para habilitar o uso do KVM.
3. No campo Diretiva de autorização do usuário, clique no botão **Habilitar tempo limite de autorização do usuário** e insira um número (em segundos) após o qual um usuário deve fornecer uma senha única para o operador do console.
4. Se você obter por não usar a opção de autorização, clique em **Desabilitar consentimento de usuário**
5. No campo **Tempo limite**, insira um número (em minutos) que uma sessão de controle remoto TCP pode ficar inativa antes que uma sessão seja encerrada. Isto é desativado se a autorização do usuário estiver desativada (passo anterior).
6. Clique em **OK**.

Restrições de KVM

- KVM não é compatível com o tipo de segurança do controle remoto.
- O tipo de segurança do controle remoto é armazenado na máquina do cliente. O servidor de autenticação pede ao cliente para retornar ao tipo de segurança e então decidir se o operador de controle remoto pode controlar a máquina do cliente remotamente. Ao conectar com o ME, não haverá nenhuma segurança ao retornar ao servidor de autenticação (servidor núcleo).
- O KVM não é compatível com as configurações da diretiva do controle remoto.
- Nenhuma diretiva "somente exibição" ou "permissão exigida" do controle remoto pode ser aplicada a conexão KVM. A opção "permissão exigida" pode ser tratada como "código de autorização do cliente exigido" em configuração de AMT e que deve ser definido na configuração do AMT em vez de no "RCViewer".
- A KVM não é compatível com as opções do controle remoto na configuração do agente
- A KVM não é compatível com os recursos transferência de arquivos, execução remota, bate-papo e desenho com a conexão KVM.
- KVM does not support the remote control blank screen option.

Diretivas de segurança de rede do Intel vPro

Intel vPro includes a System Defense feature, which enforces network security policies on managed devices. LANDesk® Management Suite applies a System Defense policy to Intel vPro devices. Each device filters incoming and outgoing network packets according to the defined policies.

Quando o tráfego na rede coincidir com as condições de alerta definidas em um filtro, um alerta é gerado e o acesso à rede do dispositivo é bloqueado. The device is then disconnected from the network until you reconnect the access using the System Defense Remediation feature.

How Intel vPro System Defense policies are applied

Quando uma diretiva de Defesa de sistema está ativa em um dispositivo gerenciado, o dispositivo monitora todo o tráfego de entrada e saída da rede. O seguinte ocorre se as condições do filtro forem detectadas:

1. O dispositivo gerenciado envia um alerta ASF ao servidor núcleo e uma entrada é acrescentada ao log de alerta.
2. O servidor núcleo determina qual diretiva foi invalidada e fecha o acesso à rede no dispositivo gerenciado.
3. O dispositivo é mostrado na fila de correção de Defesa do sistema.
4. Para restaurar o acesso do dispositivo à rede, o administrador segue as etapas necessárias de correção e, em seguida, remove o dispositivo da fila de correção; isso restaura a diretiva original de Defesa do sistema no dispositivo.

Diretivas de Intel vPro System Defense

A tecnologia Defesa de sistema Intel vPro permite à rede filtrar ao nível do chip do Intel AMT. Os sistemas que estiverem infectados e que representem uma ameaça à rede podem ser colocados em quarentena remotamente com determinadas portas e endereços de IP que permanecem abertos para a correção, sem ameaçar o resto da rede.

LANDesk Management Suite contains the following predefined System Defense policies.

- **BlockFTPSrvr:** Esta diretiva impede o tráfego através da porta FTP. Quando os pacotes são enviados ou recebidos na porta 21 do FTP, os mesmos são soltos e o acesso à rede é suspenso.

- **LDCBKillNics:** Esta diretiva bloqueia o tráfego em todas as portas da rede com exceção das seguintes portas de gerenciamento:

Descrição da porta	Número da faixa	Direção do tráfego	Protocolos
LANDesk management	9593-9595	Enviar/receber	TCP, UDP
Gerenciamento Intel vPro	16992-16993	Enviar/receber	Somente TCP
DNS	53	Enviar/receber	Somente UDP
DHCP	67-68	Enviar/receber	Somente UDP

  Quando o servidor núcleo termina o acesso à rede em um dispositivo gerenciado, ele aplica esta diretiva ao dispositivo. Em seguida, quando o dispositivo é removido da fila de correção, a diretiva original é reaplicada ao dispositivo.

- **LDCBSYNFlood:** Esta diretiva detecta um ataque de recusa de serviço SYN flood: ela não permite mais que 10.000 pacotes TCP com o sinalizador SYN ativado, em um minuto.. Quando o número é excedido, o acesso à rede é suspenso.
- **UDPFloodPolicy:** Esta diretiva detecta um ataque de recusa de serviço UDP flood: ela não permite mais que 20.000 pacotes UDP por minuto nas postas de 0-1023. Quando o número é excedido, o acesso à rede é suspenso.

Restauração de acesso à rede para dispositivos com Intel vPro

Se o acesso à rede de um dispositivo estiver suspenso por causa de uma diretiva da Defesa do sistema, o dispositivo aparece na fila de correção. Ele permanecerá lá até que você o remova da lista, o que reintegra a diretiva naquele dispositivo.

Antes de fazê-lo, é necessário resolver o problema que colocou o dispositivo na fila. Por exemplo, se o tráfego FTP foi detectado, você precisará confirmar que as ações apropriadas foram tomadas para impedir mais tráfego FTP no dispositivo.

Para restaurar o acesso a uma rede de um dispositivo na fila de correção

1. Clique em **Configurar > Opções Intel vPro > Correção da defesa do sistema**.
2. Select the devices that can have their network access restored and click **Remediate**.

This action restores network access and applies the System Defense policies to the selected devices.

Editar strings de notificação do cliente Intel vPro

Você pode enviar uma mensagem para notificar um usuário quando a Defesa de sistema Intel vPro detectar um problema e remover o dispositivo do usuário da rede. A caixa de mensagem aparece no dispositivo quando ele é desconectado da rede e uma segunda mensagem é mostrada após o problema ter sido resolvido e o dispositivo for reconectado a rede (removido da fila de correção) pelo administrador.

Use esta caixa de diálogo para inserir as strings de notificação exibidas em dispositivos gerenciados. Você pode usar uma mensagem de texto padrão ou personalizada.

Para usar notificações de mensagem para a Defesa de sistema do Intel vPro

1. Clique em **Configurar > Opções do Intel vPro > Strings de notificação do cliente**.
2. Marque a caixa **Habilitar** para enviar mensagens quando você estiver desconectado do servidor.
3. Para personalizar a mensagem, substitua o texto padrão com a mensagem que você quer exibir nos dispositivos dos clientes.
4. Clique em **OK**.

Suporte Intel vPro sem fio

Os dispositivos (versão 2.5 ou mais recente) com capacidade sem fio podem ser gerenciados fora da banda através de uma conexão LAN sem fio ao serem ligados e com a interface sem fio ativada. Se o notebook estiver no modo de descanso, poderá ser gerenciado fora da banda somente se estiver conectado a uma LAN cabeada e conectado com o cabo de energia.

Quando o notebook está ligado, o chip da tecnologia Intel Active Management Technology (Intel AMT) se comunica com o driver da LAN sem fio. Se a Intel AMT encontrar um perfil correspondente, o driver roteará o tráfego endereçado para o dispositivo Intel AMT. Mesmo se houver um problema com o driver, a Intel AMT pode receber o gerenciamento de tráfego fora da banda a partir da interface de rede sem fio.

Para o gerenciamento de rede sem fio, o Intel vPro usa o perfil de rede sem fio do Windows do dispositivo.

Para a Intel AMT trabalhar com uma conexão LAN sem fio, ela deve compartilhar o endereço IP com o notebook. Para tanto, a Intel AMT deve ser configurada para usar DHCP e deve haver um servidor DHCP disponível para alocar os endereços IP. Se a Intel AMT for configurada para usar endereços de IP estáticos, a conectividade sem fio será desativada.

Quando um notebook é descoberto e provisionado enquanto conectado a uma rede cabeada, ele pode ser gerenciado imediatamente através dela. Contudo, ao se conectar a uma conexão sem fio, pode haver um atraso entre o estabelecimento do Intel vPro no notebook. Isso acontece devido a uma alteração em como o nome do computador é resolvido em DNS na rede. O endereço IP sem fio para o notebook é diferente do endereço IP na rede cabeada, por isso há um atraso antes do novo endereço IP conseguir compatibilidade com o nome do computador.

Configuração geral do Intel vPro

A caixa de diálogo Configuração geral contém opções de configuração que você precisa configurar antes de poder gerenciar os dispositivos habilitados com Intel vPro.

NOTA: Insira uma senha nesta caixa de diálogo somente você pretende habilitar características de Intel vPro para dispositivos administrados aplicáveis. A senha é gravada na banco de dados e aplicado globalmente para dispositivos Intel vPro de Provisionamento, então você deve entender como montar e configurar cada versão de dispositivos Intel vPro.

Instalação e configuração

O diálogo Configuração geral do Intel vPro lhe permite mudar a senha usada com a conta " admin" padrão. Essa senha é aplicada a todos os novos dispositivos com Intel vPro quando você os provisiona. Você tem também a opção de mudar essa senha em todos os dispositivos com Intel vPro gerenciados no momento. Essa opção é recomendada para que todos os dispositivos tenham as mesmas credenciais.

- **Senha:** Insira uma senha segura para se comunicar para provisionar novos dispositivos Intel vPro. Para os dispositivos que você gerenciará, a senha digitada na Tela de configuração da Intel AMT (acessada no BIOS do dispositivo) deve ser a mesma digitada na caixa de diálogo Configuração geral do Intel vPro. Esta senha é salva no banco de dados e aplicada globalmente para provisionamento de dispositivos com Intel vPro.
- **Sincronizar esta senha:** Marque esta caixa para aplicar a senha a todos os dispositivos Intel vPro gerenciados.
- **Usar comunicações não-TLS:** Marque esta caixa se você escolher usar comunicações não-TLS, que são menos seguras, com dispositivos configurados usando o modo Enterprise. Esta opção não é recomendada por causa dos riscos de segurança do uso de um método de comunicação menos seguro.

Usar uma senha forte

O Intel vPro exige o uso de uma senha forte para ativar comunicações seguras. As senhas devem satisfazer aos seguintes requisitos:

- Ter pelo menos 8 caracteres
- Incluir pelo menos um número (de 0 a 9)
- Incluir pelo menos um caractere ASCII não alfanumérico (por exemplo !, &, %)
- Conter caracteres latinos maiúsculos e minúsculos ou caracteres não ASCII (UTF+00800 e acima)

Provisionamento automático para o Intel vPro 6.2 e acima

O Management Suite provisiona automaticamente dispositivos Intel vPro com versão AMT 6.2 e acima. Se você inserir uma senha nesta caixa de diálogo, mas não tiver definido uma uma PID nos dispositivos ou forneceu um certificado sem toque, seus dispositivos são provisionados usando o modo de Controle de cliente. Este modo limita algumas das funcionalidades do Intel vPro, refletindo o baixo de nível de confiança necessário para concluir a configuração do dispositivo.

Se você inserir uma senha nesta e definiu uma uma PID nos dispositivos ou forneceu um certificado sem toque, os dispositivos são provisionados usando o modo de Controle de admin, que não limita as funcionalidades do Intel vPro, refletindo um maior nível de confiança associado a configuração do dispositivo.

Tempo limite

O seu ambiente de rede pode exigir um tempo limite mais alto para as chamadas de comunicação para que haja menos erros de rede. Se você aumenta o intervalo do limite de tempo para chamadas do Intel vPro, algumas operações podem levar mais tempo para concluir se dispositivos não respondem nem não estão conectados à rede.

- **Tempo limite:** Defina o valor em segundos que o Intel vPro usará para chamadas de comunicação na rede. O valor mínimo é 5 segundos.

Configuração da detecção do ambiente de rede

Com o Acesso remoto Intel vPro, o domínio ao qual o dispositivo é conectado é considerado estar dentro da rede de empresa ou fora de empresa. Este diálogo contém domínios válidos que definem a rede da empresa.

Se um dispositivo Intel vPro (revisão 3.0 ou mais recente) é conectado a um domínio desta lista, ele pode ser gerenciado diretamente do servidor núcleo e se comunica com o núcleo através de conexões normais do Intel vPro. Se o dispositivo for conectado a qualquer outro domínio, ele só pode ser gerenciado com o uso do Acesso remoto do Intel vPro.

Como padrão, as configurações da Detecção de ambiente de rede (NED - Detecção de ambiente de rede) são aplicadas somente aos dispositivos Intel vPro que são equipados com Acesso remoto. Quando é marcada a caixa de seleção **Aplicar a configuração da NED somente a computadores configurados por Acesso remoto** as configurações são aplicadas aos dispositivos com Acesso remoto e elas são ignoradas para outros dispositivos Intel vPro.

NOTA: É necessário ter todos os domínios válidos na rede de empresa relacionados aqui. Se você não colocar todos os domínios válidos na lista, todas as comunicações de gerenciamento do Intel vPro na rede podem ser interrompidas na rede inteira.

Para adicionar um domínio à lista de domínios aprovados

1. Digite o nome do domínio na caixa de texto **Adicionar domínio aprovado**.
2. Clique em **Adicionar**.

Para remover domínios da lista de domínios aprovados

1. Selecione um ou mais domínios na lista de domínios aprovados vPro (use a combinação Ctrl+clique para selecionar múltiplos nomes).
2. Clique em **Remover**.

Configuração do Acesso remoto Intel vPro

O Acesso remoto Intel vPro é uma combinação de tecnologias de processador, melhorias de hardware, recursos de gerenciamento e tecnologias de segurança que permitem o acesso a dispositivos Intel vPro habilitados quando não estão conectados na rede da empresa. Use esta caixa de diálogo para configurar o acesso remoto aos dispositivos Intel vPro.

Configuração do Intel vPro Gateway

Use esta seção para inserir as informações de configuração sobre o servidor usado como o Servidor do Gateway Intel vPro.

- **Acesso interno do Gateway vPro**: o endereço de IP do servidor quando acessado a partir da rede da empresa
- **Endereço interno do Gateway vPro**: o endereço de IP do servidor quando acessado de fora da rede da empresa
- **Porta HTTP do Gateway vPro**: a porta usada para comunicações HTTP entre o Servidor do Gateway Intel vPro e o servidor núcleo (padrão: 8080)
- **Porta de direcionamento do Gateway vPro**: a porta que é usada para o redirecionamento IDE (padrão: 16993)
- **Porta do cliente do Gateway vPro**: a porta usada para comunicações entre o cliente gerenciado e o Servidor do Gateway Intel vPro (padrão: 20015)

Configuração da sessão periódica do Acesso remoto

Essas configurações determinam a frequência e duração as sessões de acesso remoto são abertas para manutenção de dispositivos Intel vPro.

- **Intervalo da sessão**: o número de horas entre o início de cada sessão remota. O padrão é 24 horas.
- **Duração da sessão**: a duração da sessão remota, em minutos, antes que encerre automaticamente. O padrão é 30 minutos; o mínimo é 10 minutos

Configuração do cliente de Acesso remoto

Marque a caixa **Habilitar acesso remoto em todos os clientes vPro** para ativar o acesso remoto em todos os dispositivos Intel vPro durante o gerenciamento de dispositivos. Quando ativado, os dispositivos serão conectados remotamente quando fora da rede da empresa. Se esta opção não estiver selecionada, as configurações de acesso remoto are gravadas no banco de dados não são enviadas aos dispositivos Intel vPro gerenciados.

Abrir sessões remotas de vPro

Esta sessão exibe as sessões remotas abertas nos dispositivos Intel vPro.

To end a session immediately, select the session in the list and click **End Session**.

Para reiniciar um dispositivo Intel vPro remotamente, selecione uma sessão aberta e clique em **Gerenciador de inicialização vPro**. Você pode reiniciar o dispositivo a partir do CD/DVD, do HD local, PXE ou IDE redirecionado.

Gerenciamento de dispositivos Intel vPro

Management Suite suporta dispositivos usando a tecnologia Intel vPro, uma tecnologia de hardware e firmware que permite o gerenciamento de dispositivos remotos e de segurança. A Intel vPro utiliza a comunicação fora de banda (OOB) para o acesso a dispositivos independentemente do estado do sistema operacional ou da alimentação fornecida ao dispositivo.

Neste produto, o termo "Intel vPro" refere-se a tecnologias fornecidas nos computadores desktop e portáteis com suporte para Intel vPro. Este produto também suporta dispositivos com versões anteriores da Intel AMT (Intel Active Management Technology - Tecnologia de gerenciamento ativo Intel). O processo para configuração de dispositivos com diferentes versões do Intel vPro varia de acordo com os números das versões.

Gerenciamento do dispositivo Intel vPro

Quando um dispositivo Intel vPro é adicionado ao banco de dados núcleo para ser gerenciado, ele pode ser gerenciado de forma limitada mesmo se ele não tiver um agente LANDesk instalado.

Desde que os dispositivos estejam conectados à rede e tenham uma alimentação de espera, eles podem ser descobertos e podem ser adicionados ao banco de dados para serem gerenciados com outros dispositivos na rede.

Se um dispositivo possuir a tecnologia Intel vPro, mas não um agente de gerenciamento instalado, ele poderá ser descoberto, adicionado ao banco de dados de inventário e exibido na pasta Dispositivos da visualização de rede. Os recursos de gerenciamento disponíveis para os dispositivos configurados com a tecnologia Intel vPro são:

- **Resumo de inventário:** um subconjunto dos dados de inventário normal do dispositivo poderá ser consultado e examinado em tempo real mesmo se o dispositivo estiver desligado.
- **Log de eventos:** um log com eventos específicos da Intel vPro, o qual mostra a gravidade e a descrição dos eventos, pode ser observado em tempo real.
- **Gerenciador de inicialização remota:** a ciclagem (ligar/desligar) da alimentação e várias opções de inicialização podem ser iniciadas no console de gerenciamento remoto, independente do estado do sistema operacional ou da alimentação do dispositivo. As opções disponíveis são dependentes do suporte para as opções no dispositivo. Alguns dispositivos podem não oferecer suporte a todas as opções de inicialização.
- **Defesa de sistema**: O recurso de Defesa do sistema da Intel vPro reforça as diretivas de segurança de rede nos dispositivos gerenciados.

Outras opções de gerenciamento Management Suite só estarão disponíveis quando um agente de gerenciamento estiver instalado no dispositivo.

A tabela a seguir contém as opções de gerenciamento disponíveis para um dispositivo somente Intel vPro em comparação com um dispositivo Intel vPro que possui um agente de gerenciamento Management Suite instalado.

	Somente Intel vPro	Intel vPro e agente	Somente agente
Resumo de inventário	Resumo	X	X
Log de eventos	X	X	X
Gerenciador de inicialização remota	X	X	
Histórico do inventário		X	X
Controle remoto		X	X
Bate-papo		X	X
Transferência de arquivos		X	X
Execução remota		X	X
Ativação		X	X
Encerramento		X	X
Reinicializar		X	X
Análises de inventário		X	X
Tarefas agendadas e diretivas	Limitado	X	X

	Somente Intel vPro	Intel vPro e agente	Somente agente
Opções de grupo		X	X
Execução de relatório de inventário		X	X
Alertas Intel vPro		X	X
Deteção de ambiente de rede	X	X	
Acesso remoto iniciado pelo cliente	X	X	

Acesso a dispositivos provisionados no modo Enterprise

Quando um dispositivo Intel vPro é provisionado no modo Enterprise, o servidor núcleo instala um certificado no dispositivo para proteger a comunicação. Se o dispositivo for gerenciado por outro servidor núcleo, ele deverá ser desprovisionado e, em seguida, provisionado novamente pelo novo servidor núcleo. Se isso não for feito, o acesso à Intel vPro do dispositivo não responderá porque o novo servidor núcleo não terá o certificado correspondente. Da mesma forma, se outro computador tentar acessar a funcionalidade da Intel vPro no dispositivo, ele não obterá êxito pelo mesmo motivo.

Recursos de gerenciamento do Intel vPro

Quando um dispositivo Intel vPro é adicionado ao banco de dados do inventário, diversos recursos de gerenciamento são ativados. Acesse estes recursos clicando com o botão direito no dispositivo no modo de exibição de rede e selecione opções **Opções Intel vPro**.

A ativação desses recursos estão ativados e a quantidade de dados exibidos quando você os usa dependem do provisionamento do dispositivo se uma conexão com o dispositivo está ativada. A versão do Intel vPro no dispositivo também determina quais dados são exibidos.

Status do Intel vPro

A caixa de diálogo Status do Intel vPro exibe informações atuais sobre os recursos Intel vPro que foram ativados e estão em efeito no dispositivo. Isso inclui informações gerais, configurações de energia, perfil sem fio, agent presence, desefa do sistema, detecção de ambiente de rede e configurações de acesso remoto.

Recursos não compatíveis com o dispositivo aparecem esmaecidos.

Para ver o resumo de inventário da Intel vPro para um dispositivo

1. Na tela de rede, clique com o botão direito em um dispositivo gerenciado Intel vPro.
2. Selecione **Opções do Intel vPro > Status do Intel vPro**
3. Para atualizar as informações, clique em **Atualizar**.

Log de eventos do Intel vPro

O Management Suite fornece uma tela para o log de eventos gerados pelos dispositivos Intel vPro. As configurações determinam os eventos que são capturados no log. Você pode ver a hora/data do evento, a origem do evento (coluna Entidade), uma descrição e a severidade que é determinada pelas configurações da Intel vPro (Crítica ou Não-crítica). Os dados do log também podem ser exportado em formato de valor separado por vírgula (CSV).

Para ver o log de evento da Intel vPro

1. Na tela de rede, clique com o botão direito em um dispositivo Intel vPro e selecione **Opções Intel vPro > Log de eventos do Intel vPro**.
2. Para exportar os dados em um arquivo .csv (comma-separated value), clique no botão **Exportar** na barra de ferramentas e especifique um nome de arquivo.
3. Para limpar todos os dados no log, clique no botão **Limpar** na barra de ferramentas.
4. Para atualizar as entradas de log, clique no botão **Atualizar** na barra de ferramentas.

Núcleos de rollup

Instalação de um núcleo de rollup (agrupado)

É possível usar um núcleo de rollup para combinar os dados de vários servidores núcleo. É necessário agendar atualizações do núcleo de rollup para sincronizar o banco de dados núcleo de rollup com cada banco de dados núcleo do servidor núcleo. Com o Web Console Management Suite é possível gerenciar dispositivos no núcleo de rollup por meio de consultas, da distribuição do software, do controle remoto e de outros recursos para os quais o Web Console fornece suporte.

Antes de instalar um núcleo de rollup, é necessário ter configurado um servidor de banco de dados de rollup adicional Oracle ou SQL Server. A opção de rollup do Management Suite solicitará informações sobre o banco de dados configurado.

Você pode fazer o rollup de dados dos núcleos usando a versão 8.7 SP2 ou mais recente do Management Suite. O núcleo de rollup precisa ser instalado da versão mais recente do Management Suite. Todos núcleos precisam estar usando o mesmo tipo de banco de dados como todos SQL ou todos Oracle. Se você estiver fazendo rollup de versões do Management Suite mais antigas que 9.0 e estiver usando também uma versão de byte duplo do (japonês, chinês ou russo), todos os núcleos precisam estar usando o mesmo idioma.

Para instalar um núcleo de rollup:

1. Configure um servidor para hospedar o núcleo de rollup e banco de dados.
2. Instale o banco de dados da mesma forma como faria com uma instalação normal do Management Suite. Mais informações sobre a instalação de bancos de dados estão disponíveis na comunidade LANDesk http://community.landesk.com.
3. Inicie a sessão no servidor núcleo de rollup com uma conta que tenha direitos de administrador.
4. Instale o núcleo de rollup com a execução automática na mídia de instalação do Management Suite. Finalize a instalação.

Configuração de links do banco de dados de rollup

Esta seção descreve a maneira de configurar os links de banco de dados no núcleo de rollup. Você precisa fazer isso antes de poder iniciar o rollup de dados.

A pessoa que faz a configuração deve também ter acesso a todos os DBMSs usados pela LANDesk e precisam ter permissão de segurança para criar links de banco de dados e executar as etapas de configuração no nível de servidor de DBMS.

Rollup de Oracle para Oracle

Configurar banco de dados Oracle

O arquivo TNSNames.ora no servidor de banco de dados onde o seu banco de dados de rollup existe deve conter uma entrada para o seu banco de dados do servidor núcleo.

1. No caso do banco de dados Oracle, dentro do Console do Enterprise Manager, conecte ao seu banco de dados. Expanda **Distribuído**.
2. Clique com o botão direito no item **Links de banco de dados** e clique em **Criar**.

3. No campo **Nome**, digite um nome para o link de banco de dados.
   Observação: se o banco de dados AR estiver usando Oracle9i, o nome do link pode ser qualquer nome que já não esteja em uso ou reservado. A instalação solicitará essas informações.
4. Selecione **Usuário fixo** e digite o nome de usuário e a senha para o banco de dados do servidor núcleo.
5. No campo **Nome do serviço**, digite a entrada TNSNames.ora (por exemplo, NetAlias) que se refere ao seu banco de dados do servidor núcleo.
6. Clique em **Criar**.
7. Clique duas vezes no seu link recém-criado e clique em **Testar**. Uma mensagem indicando que o seu link está ativo deverá ser exibida. Você também pode testar seu link acessando o banco de dados de rollup e emitindo o seguinte comando:
   Select count(*) from computer@linkname;
   Se o retorno for uma contagem de dispositivos no banco de dados de produção do servidor núcleo, isso significa que o link está configurado corretamente.

Rollup de SQL Server para SQL Server

Configurar banco de dados SQL Server

1. Abra o SQL Server Management Studio.
2. Expanda o seu servidor e, em seguida, **Objetos de Servidor**.
3. Clique com o botão direito em item **Servidores vinculados** e clique em **Novo servidor vinculado**.
4. Na página **Geral**, siga as etapas de 5 a 11:
5. **Servidor vinculado:** digite um nome exclusivo para esse link de banco de dados (por exemplo, Link LDMS core server1).
6. Escolha **Outra fonte de dados.**
7. Selecione **Microsoft OLE DB Provider para SQL Server**.
8. **Nome do produto**: insira o LDMS.
9. **Fonte de dados:** digite o nome do servidor do banco de dados contendo o banco de dados núcleo.
10. **String do provedor:** insira a string do provedor. Por exemplo:

    SQL Server
    provider=SQLOLEDB.1;user id=<Usuário do banco de dados do servidor núcleo>
    ** A parte do id de usuário da string do provedor é necessária na string de conexão a outro banco de dados SQL Server. **
11. **Catálogo:** digite o nome físico do banco de dados do seu servidor núcleo (por exemplo, lddb).
12. Na guia **Segurança**, selecione **Ser feito usando este contexto de segurança** e digite o nome de usuário e a senha para o banco de dados do servidor núcleo. Em seguida, clique em **OK**.
13. Clique em **Nova consulta** e digite o seguinte comando:
    Selecione count(*) em [Link name].[database name].[table-owner name].Computer
    Usando os valores acima, esta consulta apareceria como:
    Selecione contagem(*) em [LDMS Core Server1 Link].[lddb].[dbo].Computer
    Se a contagem correta voltar, o seu link está configurado corretamente.

Uso do Utilitário de rollup do banco de dados

O Utilitário rollup de banco de dados (DBRollup.exe) permite obter vários bancos de dados núcleo e combiná-los em um único banco de dados rollup núcleo de destino. O limite do dispositivo de núcleo de rollup depende do hardware e de seus níveis aceitáveis de desempenho. O banco de dados de origem pode ser um servidor núcleo ou um servidor núcleo de rollup.

Os requisitos de sistema para um banco de dados de destino podem ser superiores aos requisitos para um banco de dados padrão. Esses requisitos podem variar consideravelmente de acordo com o ambiente de rede. Se forem necessárias mais informações sobre os requisitos de hardware e software para o banco de dados de destino, entre em contato com um representante de atendimento ao cliente do software LANDesk.

O programa de instalação instala automaticamente o Utilitário de Rollup do banco de dados com o núcleo de rollup. O Utilitário de Rollup usa um mecanismo de recepção para acessar os dados nos núcleos selecionados. Para que os rollups de banco de dados funcionem, é necessário que já exista uma unidade correlacionada com cada núcleo do qual você deseja que o Utilitário de Rollup obtenha dados. A sua conta de conexão deve ter direitos de leitura do registro do servidor núcleo.

O Utilitário de Rollup verifica na chave de registro do servidor núcleo informações sobre o banco de dados e as conexões (HKLM\SOFTWARE\LANDesk\ManagementSuite\Core\Connections\local) e usa as informações dessa chave para acessar o banco de dados associado a cada núcleo adicionado ao Utilitário de Rollup. Para bancos de dados Oracle, a definição TNS no servidor do qual você está executando o Utilitário Rollup deve corresponder à definição TNS no servidor núcleo que o utilitário está acessando.

Você pode usar o Utilitário de rollup para selecionar os atributos que deseja que sejam submetidos ao rollup a partir dos núcleos. Os atributos que você selecionar aplicam-se a todos os núcleos. Limitar o número de atributos reduz o tempo de rollup e a quantidade de dados transferidos durante os rollups. Se você souber que não consultará determinados atributos, eles poderão ser removidos.

O Utilitário Rollup sempre faz o rollup dos dados com o atributo selecionado. O rollup também não inclui nenhuma consulta ou escopo que você tenha definido. Qualquer usuário do console com direitos ao banco de dados rollup terá acesso a todos os dados desse banco de dados. Você pode usar a segurança em nível de recursos para limitar o acesso aos recursos do Web Console.

Após adicionar os servidores núcleo nos quais deseja efetuar o rollup, além da lista atributos desses servidores, você pode clicar em **Agendar** para adicionar um script de rollup agendado para cada servidor núcleo. A partir de um Web Console, você poderá, então, agendar esses scripts de rollup para execução na hora e no intervalo desejados. Os scripts de rollup podem ser vistos apenas pelo Web Console, ficando residentes no núcleo de rollup.

Iniciar o utilitário de rollup

Para iniciar o Utilitário de Rollup

1. Em um núcleo de rollup, execute o Utilitário de Rollup (\Arquivos de programa\LANDesk\ManagementSuite\dbrollup.exe).
2. Selecione na lista um servidor núcleo de rollup existente para gerenciar, ou clique em **Novo** para digitar o nome de um novo servidor núcleo de rollup. Observe que é necessário digitar o nome do servidor núcleo e não o nome do banco de dados.
3. Após selecionar um núcleo de rollup, a lista **Núcleos de origem** mostrará os núcleos que você configurou para efetuar o rollup para o núcleo de rollup selecionado.

Sobre o Utilitário de Rollup

Use o Utilitário de Rollup de banco de dados (execute-o a partir do núcleo de rollup) para gerenciar rollups de dados a partir dos servidores núcleo.

- **Núcleo de rollup:** Você pode gerenciar vários núcleos de rollup com o Utilitário de Rollup. Selecione o núcleo que deseja gerenciar. Antes, uma unidade deve ser mapeada para cada núcleo de rollup.
- **Novo:** Clique para adicionar um novo núcleo de rollup que deseja gerenciar. Antes, uma unidade deve ser mapeada para o núcleo de rollup que você está adicionando. Informe o nome do computador do núcleo de rollup e clique em **OK**.
- **Atributos:** Clique para selecionar os atributos que deseja submeter ao rollup. A lista de atributos é global para todos os servidores núcleo utilizados pelo núcleo de rollup selecionado. Transfira atributos individuais ou árvores de atributos da coluna Atributos selecionados (esses atributos passarão por rollup) para a coluna Atributos disponíveis (esses atributos não passarão por rollup).
- **Redefinir o banco de dados:** Clique para redefinir o banco de dados rollup selecionado. Esta operação exclui todos os dados e reconstrói todas as tabelas.
- **Adicionar:** Clique para adicionar um núcleo a partir do qual você deseja adicionar dados no núcleo de rollup selecionado.
- **Excluir:** Clique para remover do banco de dados núcleo de rollup selecionado o núcleo selecionado e seus dados. **AVISO:** Esta opção exclui os dados do núcleo selecionado quando você clica em **OK**. Dados de outros servidores núcleo permanecem no banco de dados rollup.
- **Agendar:** Clique para adicionar um script de rollup ao núcleo selecionado. Se você não possui um núcleo selecionado na caixa Núcleos de origem, esta opção cria scripts de rollup para todos os núcleos na caixa Núcleos de origem.
- **Rollup:** Clique para efetuar um rollup imediato a partir do núcleo selecionado. É preciso selecionar um núcleo para essa opção estar disponível.
- **Fechar:** Clique para fechar o Utilitário de Rollup.

Configurar atributos agrupados (rolled-up)

Para configurar os atributos em que deseja agrupar

1. No Utilitário de agragação, selecione o núcleo de agragação que deseja configurar.
2. Clique em **Atributos**.
3. Por padrão, todos os atributos do banco de dados são submetidos a agregação. Transfira da coluna **Atributos selecionados** para a coluna **Atributos disponíveis** os atributos que você não quer submeter ao rollup.
4. Clique em **OK** quando tiver concluído. A transferência dos atributos para a coluna Atributos disponíveis exclui do banco de dados de agregação os dados associados.

Configure os servidores núcleo de origem para um núcleo de rollup

Para configurar os servidores núcleo de origem para um núcleo de rollup

1. No Utilitário de agragação, selecione o núcleo de agragação que deseja configurar.
2. Após selecionar um núcleo de rollup, a lista de núcleos de Origem mostrará os núcleos que você configurou para efetuar o rollup para o núcleo de rollup selecionado. Clique em **Adicionar** para adicionar mais núcleos ou selecione um núcleo e clique em **Excluir** para remover um deles.

AVISO: Ao clicar em **Excluir**, o núcleo selecionado juntamente com todos os dados desse núcleo é imediatamente removido do banco de dados núcleo de rollup. Além disso, se fornecer um nome de link inválido quando adicionar o servidor núcleo ao banco de dados rollup, você terá que remover o núcleo do rollup e adicioná-lo novamente a fim de modificar o nome de link.

Agendar trabalhos de rollup de banco de dados

Só é possível processar um rollup por vez. Um rollup agendado falhará se outro já estiver em andamento. Ao agendar rollups, aloque tempo suficiente entre eles de forma a não haver sobreposições. Se for difícil de predizer os horários de agendamento de rollups, é melhor agendar todos os rollups em um serviço só. Isso pode ser feito através da seleção de vários núcleos antes de clicar em **Agendar**. Dessa forma, os rollups são realizados um de cada vez, automaticamente.

AVISO: Não agende rollups de núcleos durante as horas em que eles estarão descarregando informações de patch. O download de informações de patch sobrecarrega o banco de dados e isso torna o rollup lento.

Para agendar trabalhos de rollup de banco de dados no Web Console

1. No Utilitário de Rollup, selecione o **Núcleo de rollup** que deseja configurar.
2. Na lista **Núcleos de origem**, selecione o núcleos que deseja agendar para o rollup e clique em **Agendar**. Se não nenhum núcleo for selecionado, todos os núcleos da lista serão agendados como padrão quando você clicar em **Agendar**. Clicar em **Agendar** adiciona um script de rollup do núcleo selecionado ao núcleo de rollup selecionado. Se você selecionar vários núcleos, eles serão agendados como um trabalho e serão processados um por vez.
3. No Web Console, conecte-se ao servidor núcleo de rollup.
4. No painel esquerdo de navegação, clique em **Agendar trabalhos de rollup**.
5. Clique no script de rollup que deseja agendar. Os nomes dos scripts começam com o nome do núcleo de origem, seguidos do nome do núcleo de rollup de destino entre parênteses. Clique em **Agendar rollup**.
6. Selecione quando você quer que o rollup seja realizado e se ele deve ser automaticamente reagendado ou não. Certifique-se de que somente um núcleo faça rollup por vez. Clique em **Continuar na próxima etapa**.
7. Verifique o agendamento do script e clique em **Finalizar**.

NOTA: Após o rollup dos dados dos servidores núcleo com o Management Suite de versão mais antiga que 9.0, o diálogo **Status do rollup** do DBRollup.exe mostrará que a mensagem "Tarefa terminada com um ou mais erros." Isso é normal. Além disso, se você agendar uma tarefa de rollup para um núcleo pré-9.0, a tarefa agendada mostrará a mensagem "Falha - O manipulador da tarefa encontrou um erro" mesmo que a tarefa tenha sido concluída corretamente. Isso também é normal, mas você precisa checar os logs do DBRollup e do banco de dados se suspeitar que a falha é devido a outro motivo, por exemplo, travamento do banco de dados.

Replicar dados do núcleo de rollup aos núcleos de origem

Se você tiver um núcleo de rollup no ambiente LANDesk, poderá replicar esses itens aos servidores núcleo de origem:

- Consultas
- Configurações do pacote de distribuição
- Configurações do método de entrega

Você pode criar configurações padrão para esses itens no núcleo de rollup e depois usar a replicação para torná-los disponíveis nos núcleos de origem para os seus usuários do Management Suite.

A ferramenta **Replicar aos núcleos** é visível quando o Web console estiver conectado a um núcleo de rollup. São necessários direitos de administrador LANDesk na conta para fazer a conexão. Ao clicar nessa ferramenta, aparece um diálogo onde poderá nomear a tarefa de replicação e escolher o que será replicado. Ao configurar essas informações e clicar em **OK**, aparecerá uma tarefa com o nome escolhido na tela **Tarefas agendadas** do núcleo de rollup.

A replicação não iniciará até você configurar a tarefa. A tarefa pode ser iniciada manualmente com a opção **Iniciar agora** ou você pode criar uma ação recorrente. Quando a tarefa é executada, o núcleo de rollup cria um documento XML com as informações a serem replicadas. As tarefas de replicação não são grandes ou complexas; você pode usar qualquer horário de replicação necessário para o seu ambiente de gerenciamento.

As tarefas de replicação não usam alvos selecionados manualmente. Os núcleos de origem com núcleo de rollup recebem o arquivo XML e mostram os dados replicados. Você pode usar o Utilitário de rollup do banco de dados (DBRollup.exe) para anexar os certificados do núcleo de rollup.

Somente os dados com um proprietário "Público" são replicados. Se você tiver dados que não devem ser replicados, designe-os a um proprietário que não seja "Público". Você pode editar dados replicados nos núcleos de origem, mas a não ser que modifique o nome do item, as suas mudanças serão sobregravadas na próxima replicação com um item que tiver o mesmo nome. Se os itens replicados estiverem em grupos personalizados no núcleo de rollup, a estrutura do grupo também é replicada nos núcleos de origem.

A replicação só acrescenta os dados replicados aos núcleos de origem. Se você excluir um item no núcleo de rollup que já foi replicado, a exclusão não será feita nos núcleos de origem. Se quiser excluir um item replicado nos núcleos de origem, deverá fazê-lo manualmente.

Para usar a replicação em um núcleo de rollup

1. No núcleo de rollup, configure as consultas públicas, os pacotes de distribuição e os métodos de entrega que quiser replicar.

2. Conectado ao Web console do núcleo de rollup com uma conta de administrador LANDesk, clique na ferramenta **Replicar aos núcleos**.
3. Digite um nome de tarefa e marque os itens que quiser replicar.
4. Clique em **OK**.
5. Clique na ferramenta **Tarefas agendadas**.
6. Inicie a tarefa de replicação agora ou agende-a para mais tarde. Quando a tarefa for executada, os servidores núcleo de origem com um certiticado de núcleo de rollup recebem os dados replicados.

Aumento do tempo limite do banco de dados de rollup

Com grandes bancos de dados rollup, o editor de consultas do Web Console poderá atingir o limite de tempo ao tentar exibir uma lista extensa, com a lista de Nomes de Pacotes de Software. Quando isso acontece, a lista que você está tentando exibir não mostrará nenhum dado. Se o seu limite de tempo se esgotar freqüentemente, será necessário aumentar o valor de limite de tempo do banco de dados. Isso precisa ser feito sempre que o serviço do IIS ou o servidor do Web Console for instalado. Na seguinte chave de registro:

- HKEY_LOCAL_MACHINE\SOFTWARE\LANDesk\ManagementSuite\Core

Adicione uma nova DWORD, Timeout, com um valor decimal de 1800. Esse valor é em segundos. Você pode ajustar esse valor de acordo com o tipo das suas consultas e da velocidade do banco de dados. Pare e reinicie o IIS para que a alteração tenha efeito.

Servidores preferenciais e replicação de conteúdo

Visão geral dos servidores preferenciais e replicação de conteúdo

Servidores preferenciais são uma forma do Management Suite reduzir o tráfego da rede em todas as sub-redes. Uma vez que configurados corretamente, os servidores preferenciais são incluídos na ordem de alvos de distribuição procurarão por arquivos de distribuição:

1. O cache local de distribuição do alvo.
2. Parceiros locais na mesma subrede do alvo com os arquivos de origem no seu cache de distribuição.
3. Se configurado, o servidor preferencial mais próximo.
4. A origem da distribuição, originalmente especificada no pacote de distribuição.

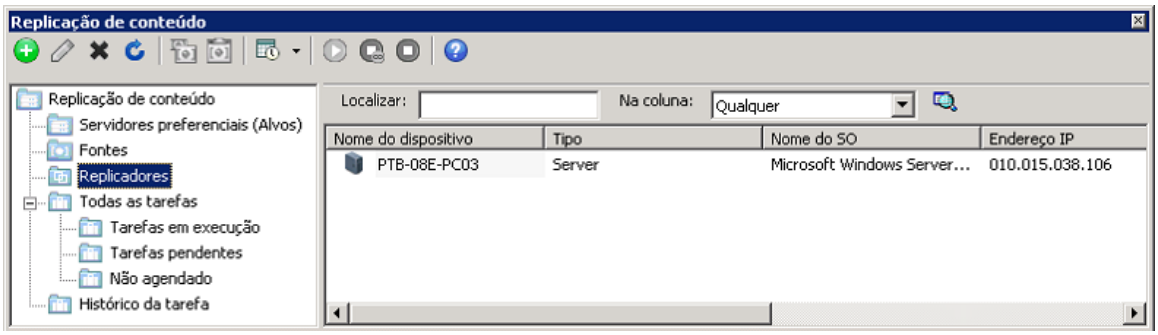
A replicação de conteúdo fornece uma estrutura de gerenciamento para estabelecer, sincronizar e atualizar os arquivos nos servidores preferenciais com aqueles no servidor de origem. Você não tem que usar a replicação de conteúdo com seus servidores preferenciais, mas usar a replicação de conteúdo permite que os administradores garantam facilmente que os arquivos nos servidores preferenciais em todo ambiente sejam mantidos até a data do agendamento pré-definido.

A replicação de conteúdo exige a configuração dos elementos a seguir:

- **Servidor preferencial:** Os alvos da distribuição tentarão baixar os arquivos de origem deste servidor. O software de distribuição pode acessar arquivos em servidores preferenciais que não foram replicados, embora a Replicação de conteúdo forneça a melhor solução para manter estes arquivos atualizados.
- **Origem:** Este é o servidor que tem os arquivos que precisam ser replicados nos servidores preferenciais. Os administradores configurarão estruturas de arquivo e arquivos na origem, em seguida, usarão a replicação de conteúdo para copiar essas hierarquias para servidores preferenciais.
- **Replicador:** Este é um dispositivo gerenciado do Windows que copia arquivos de uma origem para um servidor preferencial. Este dispositivo gerenciado deve ter uma quantia significativa de espaço em disco para que possa manter dados de todas as origens armazenadas localmente. Se um dispositivo gerenciado usado para replicação não tem espaço suficiente em disco, o replicador precisará baixar alguns arquivos da origem todas as vezes que realizar uma tarefa de replicação.

Replicadores só podem replicar conteúdo de um servidor de origem para um servidor preferencial. Os dados replicados não precisam ser constituídos somente de dados de software de distribuição, contanto que você não se importe que aqueles dados fiquem armazenados em um servidor preferencial. Por exemplo, você também pode replicar documentos e planilhas de cálculo para servidores preferenciais localizados em outras filiais.

Você pode ter tantos servidores preferenciais, origens e replicadores quanto quiser.



Configurar servidores preferenciais

Você pode especificar os servidores preferenciais onde os dispositivos procurarão os pacotes de software de distribuição. Isso pode ser importante nos ambientes WAN de baixa velocidade onde não é desejado que os dispositivos descarreguem pacotes de servidores fora do local. Quando especificar servidores preferenciais, poderá também especificar as credenciais que os dispositivos gerenciados devem usar para se autenticarem com cada servidor preferencial. Também é possível especificar os intervalos de endereço IP para as quais o servidor preferencial estará disponível.

Quando usar servidores preferenciais com uma tarefa de distribuição, somente a porção do servidor do caminho de arquivo/pacote UNC ou URL é substituída. O resto do caminho deve ser o mesmo especificado na tarefa de distribuição. Se o arquivo não estiver no servidor preferencial ele será descarregado do local especificado no pacote de distribuição. Multidifusão (somente cache) é o único método de distribuição que não suporta servidores preferenciais. O pacote UNC compartilha o trabalho com todos os pacotes. O pacote de HTTP compartilha apenas o trabalho com os pacotes MSI e SWD.

O servidor núcleo usa hashes para verificar pacotes de distribuição nas tarefas agendadas. O servidor núcleo gerará primeiro estes hashes a partir de um servidor preferencial. O uso de um servidor preferencial local torna o processo de hashing muito mais rápido. Se o pacote não estiver disponível em um dos servidores preferenciais, o servidor núcleo gera o hash de pacote do caminho especificado no pacote de distribuição. Em geral não é aconselhável a recepção de um pacote grande pelo servidor núcleo usando um link de WAN para hashing, de forma que os arquivos de hash em um servidor que é local ao núcleo será muito mais rápido e usará menos largura de banda.

Os dispositivos gerenciados armazenam a lista do servidor preferencial localmente, no arquivo preferredserver.dat. Para criar esse arquivo, um dispositivo se comunica com o servidor núcleo e, em seguida, cria uma lista filtrada dos servidores preferenciais (baseado nos limites de intervalo do endereço IP, se houver). O dispositivo então faz uma checagem da largura de banda a cada servidor preferencial e salva os três primeiros servidores no arquivo preferredserver.dat. Observe que a checagem da largura de banda não produz resultados confiáveis ou garantidos. Por exemplo, um servidor que estiver próximo pode ter uma alta carga no momento das checagens de agente. Ele pode ser removido da lista mesmo sendo geralmente o melhor candidato.

O agente de distribuição atualiza o arquivo preferredserver.dat a cada 24 horas ou quando há mudança no endereço IP. Esse processo não é aplicado a todos os dispositivos. Os dispositivos compartilham suas listas de servidores preferenciais com os parceiros. Esse é o processo dos dispositivos gerenciados para manter uma lista atual de servidores preferenciais:

1. Se o preferredserver.dat estiver no cache local de arquivos, ele é usado pelo agente de distribuição.
2. Se o preferredserver.dat estiver em um parceiro, o agente carrega o arquivo daquele parceiro.

3. Se o preferredserver.dat não estiver disponível localmente ou em um parceiro, o dispositivo contata o servidor núcleo, cria uma lista filtrada de servidores preferenciais e a salva localmente como preferredserver.dat.
4. Se o preferredserver.dat estiver vazio ou se nenhum dos servidores preferenciais responder, o agente procura uma lista de servidor preferencial no registro local.

Se nenhuma dessas etapas resultar em um servidor preferencial, o agente local usa o caminho de distribuição especificado na tarefa de distribuição.

Configurar servidores preferenciais

Você pode especificar os servidores preferenciais onde os dispositivos procurarão os pacotes de software de distribuição. Isso pode ser importante nos ambientes WAN de baixa velocidade onde não é desejado que os dispositivos descarreguem pacotes de servidores fora do local. Quando especificar servidores preferenciais, poderá também especificar as credenciais que os dispositivos gerenciados devem usar para se autenticarem com cada servidor preferencial. Também é possível especificar os intervalos de endereço IP para as quais o servidor preferencial estará disponível.

Para configurar servidores preferenciais

1. Clique em **Ferramentas> Distribuição> Replicação de conteúdo > Servidores preferenciais**.
2. Na árvore **Replicação de conteúdo**, clique com o botão direito em **Servidores preferenciais (Alvos)** e clique em **Novo servidor preferencial**.
3. Na página Configuração, digite as informações do servidor e credenciais de somente-leitura. Clique em **Testar credenciais** para verificar se as credenciais fornecidas são válidas.
4. Na página de intervalos de endereço IP, digite os intervalos de endereço IP que este servidor preferencial deve permitir acesso.
5. Nas páginas **Replicadores selecionados**, selecione o replicador, as opções de execução e o agendamento. Clique em **Ajuda** em todas página para obter mais informações.
6. Na página **Origens**, selecione os caminhos de origem que serão replicados.
7. Na pagina **Gravar credenciais**, digite as credenciais que o replicador deve usar para gravar arquivos replicados nos servidores alvo preferenciais. Clique em **Testar credenciais** para verificar se as credenciais fornecidas são válidas.
8. Clique em **Salvar**.

Armazenamento de servidores de pacote preferencial no registro

Se quiser configurar uma lista fallback dos servidores preferenciais que serão usados se não houver servidores no arquivo preferredserver.dat file, crie a seguinte chave de registro nos dispositivos gerenciados e configure o valor ao nome do servidor preferencial de pacotes. Você pode especificar múltiplos servidores de pacotes separando-os com ponto e vírgula.

- HKEY_LOCAL_MACHINE\Sof-tware\LANDesk\ManagementSuite\WinClient\SoftwareDistribution\PreferredPackageServer

Aqui está um exemplo da entrada de registro:

- [HKEY_LOCAL_MACHINE\SOFTWARE\LANDesk\ManagementSuite\WinClient\SoftwareDistribution]

"PreferredPackageServer "="Server1;Server2;Server3"

Personalização do número de servidores armazenados no arquivo preferredserver.dat

Por padrão, o arquivo preferredserver.dat contém três servidores cujos resultados de teste dão a mais alta largura de banda durante a checagem, em ordem. Para mudar o número de servidores armazenados no arquivo preferredserver.dat, atualize a seguinte linha no arquivo ntstacfg.in# na pasta ldlogon do servidor núcleo. Os números válidos variam de 0 a 7. Quando tiver atualizado esse arquivo, as mudanças se tornam parte das configurações novas ou atualizadas de agente. É necessário redistribuir a configuração de agente aos dispositivos para que a mudança entre em efeito.

```
; Configurações para os arquivos lddwnld/ldredirect, o DynamicPreferredServers é o
; número máximo de servidores preferenciais que serão armazenados. Defina como 0 para desativar
; a funcionalidade dinâmica do servidor preferencial.
REG51=HKEY_LOCAL_MACHINE,
SOFTWARE\LANDesk\ManagementSuite\WinClient\SoftwareDistribution\DynamicPreferredServers, 3, , REG_DWORD
```

Personalização da prioridade de servidores preferenciais

Para impedir atrasos quando a maioria dos servidores preferenciais não tiverem um pacote, a lógica de redireção preferirá servidores que tenham fornecido arquivos ao dispositivo. Para mudar a prioridade de servidores preferenciais no arquivo preferredserver.dat, atualize essas linhas no arquivo ntstacfg.in# na pasta ldlogon do servidor núcleo:

```
; Para impedir atrasos quando a maioria dos servidores preferenciais não tiverem um pacote
; a lógica de redireção preferirá servidores que tenham
; fornecido arquivos ao cliente. As seguintes opções de registro controlam quando um
; servidor move para cima na lista. O valor ServerHistoryUseCount indica o número
; de vezes que um servidor deve ser usado antes de ser movido para o início da lista,
; o valor ServerHistoryCacheTime indica quanto tempo deve ser lembrado (em segundos).
REG52=HKEY_LOCAL_MACHINE,
SOFTWARE\LANDesk\ManagementSuite\WinClient\SoftwareDistribution\ServerHistoryUseCount, 3, , REG_DWORD
REG53=HKEY_LOCAL_MACHINE,
SOFTWARE\LANDesk\ManagementSuite\WinClient\SoftwareDistribution\ServerHistoryCacheTime, 3600, , REG_
DWORD
```

Autenticação UNC

Ao adicionar servidores preferenciais (**Ferramentas> Distribuição > Replicação de conteúdo > Servidores preferenciais**), você também fornece credenciais que deverão ser usadas pelos dispositivos ao acessar o servidor preferencial. Por razões de segurança, certifique-se de que essas credenciais sejam divididas entre somente leitura e acesso de gravação (para obter mais informações, consulte "Sobre a caixa de diálogo Propriedades dos servidores preferenciais" na página 874). Os dispositivos gerenciados obtêm essas credenciais de somente leitura no núcleo e as usam para fazer a autenticação no servidor preferencial quando fizer um download de arquivo.

Ao usar servidores preferenciais acrescentados à caixa de diálogo **Credenciais do servidor**, não há mais necessidade de configurar os compartilhamentos de pacote aos compartilhamentos de sessão nula, como era requerido nas versões anteriores. Contanto que as credenciais fornecidas para o servidor preferencial funcionem com o compartilhamento de pacote (Clique em **Testar credenciais** na caixa de diálogo **Nome de usuário e senha**), os dispositivos gerenciados deverão ser capazes de acessar o compartilhamento.

Configurar origens e espelhamento

Um servidor de origem armazena os arquivos que devem ser replicados para um servidor preferencial. Você pode ter quantos servidores de origem quiser. Você deverá fornecer credenciais de somente leitura no servidor de origem. No servidor de origem, desative a autenticação anônima para garantir que as credenciais de somente leitura trabalham com a autenticação padrão do Windows.

Ao replicar arquivos de servidores de origem, você tem duas escolhas de como manejar os arquivos existentes no compartilhamento de destino do servidor preferencial:

1. Deixe os arquivos existentes no compartilhamento sozinhos e apenas copie os arquivos novos/alterados.
2. Ative o espelhamento para copiar arquivos novos/alterados e, em seguida remova os arquivos existentes do compartilhamento do servidor preferencial que não estão no servidor de origem.

Seja cuidadoso se escolher ativar o espelhamento. Arquivos existentes que não estão no servidor de origem para este compartilhamento serão excluídos. Certifique-se de mover todos os arquivos importantes que existam somente no compartilhamento do servidor antes de habilitar o espelhamento.

Alem disso, se você ativar o espelhamento,certifique-se de que exista somente uma origem de dados para replicação para o compartilhamento espelhado. Se múltiplas origens são replicadas para um compartilhamento espelhado, eles entrarão em conflito, porque a replicação espelhada excluirá os dados que não fazem parte do espelho.

Para ativar o espelhamento de uma origem

1. Clique em **Ferramentas> Distribuição> Replicação de conteúdo > Servidores preferenciais**.
2. Na árvore **Origem**, clique com o botão direito do mouse na origem que você deseja espelhar e clique em **Propriedades**.
3. Na página **Espelhamento**, selecione **Ativar espelhamento**.
4. Clique em **Salvar**.

Usar um representante de origem

Um representante de origem é um dispositivo gerenciado do Windows que faz a indexação de arquivos no servidor de origem. Os representantes de origem são uma parte opcional da replicação de conteúdo. Se seu servidor de origem tem milhares de arquivos, o replicador por levar algum tempo para indexar os arquivos sozinho, especialmente se esse replicador não tiver uma conexão de baixa-latência com a origem. Neste caso, a designar um dispositivo gerenciado do Windows, que esteja próximo ou no servidor de origem, para ser um representante de origem pode acelerar as replicações, porque o replicador pode obter o rapidamente o índice de arquivos do representante da origem.

Qualquer dispositivo gerenciado do Windows pode ser o representante da origem. Não precisa ser um computador dedicado nem um servidor. Para ser eficaz, deve ser capaz de estabelecer uma conexão de baixa-latência e alta velocidade com o servidor de origem. Se o servidor de origem é um dispositivo gerenciado do Windows (e não um dispositivo SAN ou de Linux, por exemplo), o representante de origem pode estar no servidor de origem.

O representante de origem usa as credenciais de servidor de origem especificadas para construir um arquivo XML contendo informações sobre todos os arquivos no compartilhamento de origem. Cria este aquivo por demanda, mas não mais de uma vez por hora. Não é necessário mapear manualmente uma unidade no servidor de origem e nem criar nenhuma conexão de rede com servidor de origem. Isto será resolvido automaticamente pelos agentes de gerenciamento.

Quando uma tarefa de replicação que usa um representante de servidor é iniciada, o replicador usará o arquivo XML do representante de origem para decidir quais arquivos devem ser replicados. O envolvimento de representante de origem na tarefa replicação acontece uma vez que o arquivo XML é transferido para o replicador.

Atribuir um representante da origem

Um representante de origem é um dispositivo gerenciado do Windows que faz a indexação de arquivos no servidor de origem. Os representantes de origem são uma parte opcional da replicação de conteúdo. Se seu servidor de origem tem milhares de arquivos, o replicador por levar algum tempo para indexar os arquivos sozinho, especialmente se esse replicador não tiver uma conexão de baixa-latência com a origem. Neste caso, a designar um dispositivo gerenciado do Windows, que esteja próximo ou no servidor de origem, para ser um representante de origem pode acelerar as replicações, porque o replicador pode obter o rapidamente o índice de arquivos do representante da origem.

Qualquer dispositivo gerenciado do Windows pode ser o representante da origem. Não precisa ser um computador dedicado nem um servidor. Para ser eficaz, deve ser capaz de estabelecer uma conexão de baixa-latência e alta velocidade com o servidor de origem. Se o servidor de origem é um dispositivo gerenciado do Windows (e não um dispositivo SAN ou de Linux, por exemplo), o representante de origem pode estar no servidor de origem.

Atribuir um representante da origem

1. Clique em **Ferramentas> Distribuição> Replicação de conteúdo > Servidores preferenciais**.
2. Na árvore **Origens**, clique com o botão direito na origem para a qual você quer um representante e clique em **Propriedades**.
3. Na página **Representante de origem**, selecione o dispositivo que será o representante de origem e clique no botão **Selecionar**. Certifique-se de ter o dispositivo correto, você pode verificar os atributos do dispositivo na parte inferior da página ou clique em **Inventário** para ver o inventário do dispositivo.
4. Clique em **Salvar**.

Designar um replicador

Um replicador é um dispositivo gerenciado do Windows que copia arquivos de um servidor de origem para um servidor preferencial. Este replicador deve ter uma quantia significativa de espaço em disco para que possa manter dados de todas as origens de distribuição armazenados localmente no cache de distribuição do software. Se não houver espaço suficiente em disco, o replicador poderá precisar baixar alguns arquivos de origem odas as vezes que realizar uma tarefa de replicação. Cada replicador pode replicar múltiplas origens para múltiplos servidores preferenciais.

Para designar um replicador

1. Clique em **Ferramentas> Distribuição> Replicação de conteúdo > Servidores preferenciais**.
2. Clique com o botão direito na árvore do **Replicador** e clique em **Propriedades**.

3. Na página **de Identificação** , selecione o dispositivo que você quer ser um replicador e clica o botão **Seleto**. Certifique-se de ter o dispositivo correto, você pode verificar os atributos do dispositivo na parte inferior da página ou clique em **Inventário** para ver o inventário do dispositivo.
4. Clique em **Salvar**.
5. Na árvore do **Replicador**, clique com o botão direito no novo replicador e em **Aplicar configurações agora**.

Você também pode designar um replicador rapidamente arrastando um dispositivo da árvore **Tela de rede** para a árvore **Replicadores** da janela replicação de conteúdo.

NOTA: Certifique-se de que o nome de compartilhamento nos servidores preferenciais e de origem são o mesmo. Por exemplo, se o nome do compartilhamento no seu servidor de origem é shareddata, o nome do compartilhamento de destino no servidor preferencial deve ser shareddata também. Os replicadores criarão as pastas necessárias com base no nome do compartilhamento, mas um replicador não pode criar o compartilhamento.

Isto é necessário porque que quando os dispositivos gerenciados usam um servidor preferencial para baixar pacotes de arquivos, somente o novo do servidor no caminho completo do arquivo será substituído. O restante do caminho, começando pelo nome de compartilhamento, permanece como no pacote de distribuição original.

Agendar replicações

A replicação não iniciará até você agende uma tarefa de replicação. As tarefas de replicação são diferentes das tarefas de distribuição de software. Você só pode agendar tarefas de replicação a partir do painel **Replicação de conteúdo**.

É possível agendar uma tarefa de replicação por demanda ou recorrentes. Tarefas de replicação de uma única execução são boas para testar a replicação e para a configuração inicial dos servidores para a replicação.

Recomendamos que, quando a configuração de replicação estiver em funcionamento, sejam usadas tarefas de replicação recorrentes configuradas a partir das propriedades do servidor preferencial ou do replicador para automatizar a replicação. Em seguida, você pode exibir os sós da árvore de tarefas do painel **Replicação de conteúdo** para exibir os horários de replicação, o progresso e o status.

NOTA: É possível agendar a replicação a partir de um servidor preferencial ou de um menu de atalho do replicador.

Para iniciar uma tarefa de replicação de conteúdo imediatamente

1. Clique em **Ferramentas> Distribuição> Replicação de conteúdo > Servidores preferenciais**.
2. Clique na árvore **Replicadores**, clique com o botão direito do replicador que você quer agendar e clicar **Iniciar replicação de conteúdo agora**.
3. Monitore o status da replicação na caixa de diálogo status exibida.

Para agendar uma tarefa de replicação de conteúdo

1. Clique em **Ferramentas> Distribuição> Replicação de conteúdo > Servidores preferenciais**.
2. Clique na árvore **Replicadores**, clique com o botão direito do replicador que você quer agendar e clique em **Agendar replicação de conteúdo**.

3. Uma nova tarefa agendada é exibida no painel **Tarefas agendadas**.
4. Configure a nova tarefa agendada clicando com o botão direito e clicar em **Propriedades**.
5. A tarefa será executada na hora configurada.

Para agendar uma tarefa recorrente de distribuição de software

1. Clique em **Ferramentas> Distribuição> Replicação de conteúdo > Servidores preferenciais**.
2. Clique na árvore **Replicadores**, clicando no botão direito do replicador que você quer agendar e clicar em **Propriedades do replicador**.
3. Na árvore, clique em **configurações** e em seguida clique em **Agendar**.
4. Na barra de ferramentas, clique em .
5. Configure o horário desejado. Para obter mais informações, consulte "Sobre a página Agendar do replicador selecionado." na página 877.
6. Clique em **Salvar** para sair das caixas de diálogo.

Para excluir uma tarefa de replicação recorrente

1. Clique em **Ferramentas> Distribuição> Replicação de conteúdo > Servidores preferenciais**.
2. Clique na árvore **Replicadores**, clique com o botão direito no replicador que você deseja agendar e clique em **Propriedades**.
3. Na árvore, clique em **configurações** e em seguida clique em **Agendar**.
4. Selecione o agendamento que você quer excluir e na barra de ferramenta clique em .

Atualizar configurações de replicação

Os replicadores sempre verificam se existem novas configurações antes de iniciar a operação. Se você alterar as configurações em um replicador mas mantem o mesmo agendamento, o replicador receberá as configurações atualizadas automaticamente na próxima execução. No entanto, se você alterar o horário da replicação, o replicador não receberá as alterações até que o tempo de execução originalmente agendado seja atingido.

Por exemplo, se um replicador foi originalmente agendado para executar uma vez por mês e, mais tarde, você muda o agendamento para uma vez por semana, a alteração no agendamento semanal poderá legar um mês inteiro para atualizar.

Ao alterar o agendamento da replicação, você deveria agendar uma tarefa aplicar configurações subsequente para atualizar o novo agendamento e as configurações do replicador.

Para atualizar as configurações de replicação imediatamente

1. Clique em **Ferramentas> Distribuição> Replicação de conteúdo > Servidores preferenciais**.
2. Na árvore, clique com o botão direito no servidor preferencial, origem ou replicador que você deseja atualizar e clique em **Aplicar configurações agora**.

Monitoramento do andamento da replicação

Você pode monitorar o andamento da tarefa de replicação, status e histórico na exibição de árvore do painel **Replicação de conteúdo.** A exibição da árvore tem os seguintes nós:

- **Todas as tarefas:** Um resumo de todas as tarefas de replicação em execução, pendentes e não agendadas.
  - **Tarefas em execução:** Tarefas de replicação ativas.
  - **Tarefas pendentes:** As tarefas de replicação que estão agendadas para execução.
  - **Não agendada:** As tarefas de replicação que não estão agendadas para execução.
- **Histórico das tarefas:** As tarefas de replicação concluídas.

A exibição das tarefas mostra somente o status das tarefas mais recentes. Não exibirá o histórico completo das tarefas porque em muitos ambientes, a replicação pode acontecer com tanta frequência que um registro completo seria impossível de gerenciar.

Ajuda da replicação de arquivos

Sobre a caixa de diálogo Propriedades dos servidores preferenciais

Use a caixa de diálogo Propriedades dos servidores preferenciais para configurar seu servidores preferenciais Para obter mais informações, consulte "Servidores preferenciais e replicação de conteúdo" na página 866.

Para abrir a caixa de diálogo Propriedades dos servidores preferenciais

1. Clique em **Ferramentas > Distribuição > Replicação de conteúdo / Servidores preferenciais**.
2. Na árvore **Replicação de conteúdo**, clique com o botão direito em **Servidores preferenciais (Alvos)** e clique em **Novo servidor preferencial**. Você também pode clicar com o botão direito em um servidor preferencial existente e em **Propriedades**.

Sobre a página Configuração

Use a página **Configuração** para especificar o nome do servidor preferencial e as credenciais de somente-leitura. Os dispositivos gerenciados usarão essas informações para a conexão com o servidor preferencial.

- **Nome do servidor:** O nome do computador resolvível do servidor.
- **Descrição:** A descrição de servidor. Isso aparece na coluna **Detalhes** na árvore **Replicadores**.
- **Nome de usuário:** O nome de usuário somente-leitura para acessar o servidor.
- **Senha:** A senha para o nome de usuário digitado.
- **Confirmar senha:** Digite novamente a senha do usuário especificado.
- **Testar credenciais:** Testa as credenciais para verificar se são válidas no servidor.

Sobre a página Intervalos de endereços IP.

Usa a página **Intervalos de endereços IP** para inserir os valores de IP inicial e final. Somente os dispositivos dentro deste intervalo podem tentar fazer download deste servidor. Você pode digitar diversos intervalos de endereços IP.

- **Endereço IP inicial:** O endereço IP inicial do intervalo.
- **Endereço IP inicial:** O endereço IP final do intervalo.
- **Adicionar:** Adiciona o intervalo de endereços IP à lista.
- **Excluir:** Exclui o intervalo de endereço de IP selecionado.

Sobre a página replicador selecionado

Use a página replicador selecionado para selecionar o dispositivo gerenciado do Windows que você deseja que seja o replicador. Um replicador é responsável pela cópia dos dados de um servidor de origem para o servidor algo preferencial.

- **Selecionar:** Selecione o dispositivos que você deseja que seja um replicador e clique em **Selecionar** para designá-lo como o replicador.
- **Inventário:** Assim que o replicador estiver selecionado, você pode clicar neste botão para exibir o inventário do dispositivo e verificar se este é o dispositivo desejado.
- **Limpar:** Desmarca o dispositivo como um replicador.

Sobre a página Credenciais de gravação

Use a página **Credenciais de gravação** para especificar as credenciais de gravação do servidor preferencial. O replicador usará essas credenciais para conectar com o servidor preferencial para poder replicar arquivos novos ou alterados em um servidor preferencial.

- **Nome de usuário:** O nome de usuário com permissões de gravação para acessar o servidor.
- **Senha:** A senha para o nome de usuário digitado.
- **Confirmar senha:** Digite novamente a senha do usuário especificado.
- **Testar credenciais:** Testa as credenciais para verificar se são válidas no servidor.

Sobre a página Origem

Use a página **Origem** para configurar os caminhos que você deseja copiar para os servidores preferenciais.

- **Lista de caminhos de origem:** Exibe as origens que você configurou. Selecione uma origem desta lista.
- **Incluir:** Adiciona a origem selecionada à lista **Caminhos de origem incluídos**. Quando a origem estiver na lista **Caminhos de origem incluídos**, seu conteúdo será replicado para o servidor preferencial que você estiver configurando no momento em que a tarefa de replicação for executada.
- **Novo:** Abre a caixa de diálogo .Propriedades da nova origem para que você configure a nova origem, se ela não estiver configurada.
- **Excluir:** Remove a origem selecionada à lista **Caminhos de origem incluídos**.
- **Lista de caminhos de origem incluídos:** Exibe as origens cujo conteúdo será replicado para o servidor preferencial que está sendo configurado.

Sobre a caixa de diálogo Propriedades do replicador

Use a caixa de diálogo **Propriedades do replicador** para configurar um replicador.

Sobre a página Identificação

Use a página identificação para selecionar o dispositivo gerenciado do Windows que você deseja que seja o replicador. Um replicador é responsável pela cópia dos dados de um servidor de origem para o servidor algo preferencial.

- **Selecionar:** Selecione o dispositivos que você deseja que seja um replicador e clique em **Selecionar** para designá-lo como o replicador.
- **Inventário:** Assim que o replicador estiver selecionado, você pode clicar neste botão para exibir o inventário do dispositivo e verificar se este é o dispositivo desejado.
- **Limpar:** Desmarca o dispositivo como um replicador.

Sobre a página Servidores preferenciais (Alvos)

- Lista **Servidores preferenciais**: Exibe todos os servidores preferenciais que foram configurados. Move os servidores desta lista para lista **Servidores incluídos**.
- **Incluir:** Move o servidor preferencial selecionado da lista **Servidor preferencial** para a lista **Servidores incluídos**.
- **Excluir:** Move o servidor preferencial selecionado da lista **Servidores incluídos** para a lista **Servidores preferenciais**.
- Lista **Servidores incluídos**: Servidores preferenciais nesta lista serão algos para o replicador que você está configurando.

Sobre as páginas Configurações do replicador selecionado.

Use as páginas de configurações do replicador selecionado para configurar as opções de execução e agendamento do replicador.

Sobre a página Configurações

Use a página Configurações para exibir o número de revisão das configurações e o número da última revisão real informada pelo replicador.

- **Revisão atual das configurações:** Exibe o número da versão atual do produto. Todas as vezes que as configurações do replicador são alteradas e salvas, a **Revisão atual das configurações** é acrescida de um.
- **Última versão aplicada pelo replicador:** Todas as vezes que o replicador é executado, ele busca por configurações atualizadas e, em seguida informa o número de revisão das configurações usado.
- **Relato mais recente:** Exibe a data e hora que o replicador foi executado pela última vez.

Sobre a página Opções de execução do replicador selecionado

Use a página Opções de execução do replicador selecionado para configurar as opções de execução, tais como largura de banda e configurações da interface do usuário

- **Configurações da largura de banda WAN:** Ajusta a prioridade desta tarefa específica acima de outro tráfego de rede. Quanto mais alta for a porcentagem do deslizador, maior será a quantidade de largura de banda usada por esta tarefa acima de qualquer outro tráfego. As conexões WAN em geral são mais lentas, por isso recomenda-se com frequência colocar este deslizador na porcentagem mais baixa.
- **Configurações da largura de banda LAN:** Ajusta a prioridade desta tarefa específica acima de outro tráfego de rede. Quanto mais alta for a porcentagem do deslizador, maior será a quantidade de largura de banda usada por esta tarefa acima de qualquer outro tráfego. As conexões de LAN são, em geral, mais rápidas que as conexões WAN, por isso recomendada-se frequentemente que o slider seja definido em uma porcentagem mais alta que a WAN.
- **Mostrar diálogo de andamento:** Exibe uma caixa de diálogo de progresso no replicador. Quando desativado, a tarefa é executada em segundo plano sem nenhuma notificação ou indicador de status.
- **Permitir o download por parceiro:** Quando selecionado, o replicador procurará primeiro nos parceiros locais os arquivos de origem que estão sendo replicados . Se o replicador não puder encontrar o arquivo em um parceiro, ele buscará o arquivo no servidor de origem. Esta opção pode reduzir a carga de tráfego no servidor de origem.

- **Limitar o número de dias que os arquivos são mantidos em cache:** Arquivos replicados ficarão no cache local de distribuição no replicador. Ao manter os arquivos armazenados, o replicador não deve transferir arquivos do servidor de origem para cada tarefa de replicação. Se por alguma razão você quiser forçar o replicador a atualizar os arquivos armazenados periodicamente, selecione esta opção e digite o número de dias.

  Geralmente, é seguro deixar esta opção desmarcada, desde que todos os arquivos que mudem na origem sejam automaticamente atualizados no cache local na próxima vez que a tarefa de replicação for executada.
- **Configurações da largura de banda WAN:** Selecione esta opção se você quiser usar as configurações de largura de banda WAN ao enviar arquivos aos alvos.
- **Configurações da largura de banda LAN:** Selecione esta opção se você quiser usar as configurações de largura de banda LAN ao enviar arquivos aos alvos.

Sobre a página Agendar do replicador selecionado.

Use a página **Agendar** do replicador selecionado para agendar a execução do replicador. Clicar no botão adicionar exibe a caixa de diálogo Agendar replicação de conteúdo. O cronograma que você configurou é exibido na caixa de listagem Agenda. Você pode editar ou excluir um agendamento selecionando-o e clicando no botão apropriado.

Sobre a caixa de diálogo Agendar replicação de conteúdo

- Hora:
  - **Iniciar:** Clique esta opção para exibir um calendário onde pode selecionar o dia que você quer que a tarefa inicie. Uma vez escolhido o dia, você pode também digitar uma hora do dia. Estas opções são definidas à data e hora atual.
  - **Repetir depois de:** Se desejar a tarefa recorrer, clique na caixa de listagem e selecione **minutos**, **horas**, ou **dias**. Em seguida na primeira caixa digite o tempo de duração que deseja para o intervalo selecionado .
  - **Semanalmente entre:** Se desejar que a tarefa execute em dias específicos da semana, selecione os dias de início e final.
  - **Mensalmente entre:** Se desejar que a tarefa execute em datas específicas do mês, selecione as datas de início e final.
- Duração máxima:
  - **Executar até que a replicação seja concluída:** Quando selecionado, a tarefa de replicação é executada até terminar.
  - **Encerrar após:** Quando selecionado, a replicação é interrompida quando o tempo que você determinou terminar. Na próxima replicação agendada a tarefa continuará de onde parou. Esta opção pode ser útil quando você está replicando em uma conexão lenta a noite e você não quer que o tráfego da replicação interfira no tráfego da rede durante o expediente.
- Selecione o servidores preferenciais para atualizar:
  - **Atualizar todos os servidores preferenciais associados:** A replicação ocorrerá para todos os servidores preferenciais associados com este replicador.
  - **Atualize somente os servidores preferenciais a seguir:** A replicação ocorrerá somente para os servidores preferenciais selecionados. Use esta opção se você quiser agendar a replicação em horários diferentes para servidores preferenciais diferentes.

Sobre a caixa de diálogo Agendar tarefa de replicação de conteúdo

Use a caixa de diálogo **Agendar tarefa de replicação de conteúdo** para agendar uma tarefa de replicação única. Após criar uma tarefa agendada nesta caixa de diálogo, é necessário definir o horário de execução com a ferramenta **Tarefas agendadas**.

- **Nome da tarefa:** O nome desta tarefa, que é exibido na ferramenta Tarefas agendadas.
- **Criar uma tarefa agendada:** Cria uma tarefa agendada.
- **Criar uma diretiva:** Cria uma diretiva.
- **Adicionar replicadores selecionados (ou implícitos) à lista alvo:** Se você selecionou um replicador ou um servidor preferencial, esta opção não estará disponível. Em seguida, essa opção adicionará como tarefas alvo, o replicador selecionado e todos os replicadores adicionais mencionados nas configurações dos servidores preferenciais associados.
- **Replicar somente para os servidores preferenciais selecionados:** Se você selecionou um replicador, esta opção estará disponível. Esta opção cria uma tarefa que tem como alvo somente os replicadores selecionados.

Sobre a tarefa Agendar "aplicar configurações"

Use a tarefa Agendar "aplicar configurações" para atualizar o replicador com as novas configurações. Acesse esta caixa de diálogo a partir da barra de ferramentas **Replicação de conteúdo**. Os replicadores procuram automaticamente por configurações atualizadas antes de iniciar a replicação. A tarefa "aplicar configurações" é útil após a definição de um computador como novo replicador. Agendar esta tarefa instalará o software de replicação no computador.

- **Nome da tarefa:** O nome desta tarefa, que é exibido na ferramenta Tarefas agendadas.
- **Criar uma tarefa agendada:** Cria uma tarefa agendada.
- **Criar uma diretiva:** Cria uma diretiva.
- **Não adicione nenhum replicador a essa tarefa:** Deixa a lista alvo em branco para que você possa adicionar seus próprios replicadores alvo na ferramenta Tarefas agendadas.
- **Adicionar todos os replicadores desatualizados:** Adiciona todos os replicadores que apresentem uma versão de configuração anterior a mais recente.
- **Adicione somente replicadores que não tenham exibido informações (replicadores novos) :** Adiciona replicadores recentemente designados que nunca exibiram informações nem foram executados. Isso configura os novos replicadores com as últimas configurações.

Gerenciamento de ocupantes

Visão geral do Gerenciamento de ocupantes

Gerenciamento de ocupantes é um suplemento do LANDesk Management Suite que é vendido separadamente. O gerenciamento de ocupantes permite que você compartimente os dispositivos gerenciados e configurações por empresa. Se você é responsável para gerenciar múltiplas companhias ou organizações distintas dentro da própria empresa, antes você teria que distribuir servidores núcleo do LANDesk Management Suite para cada local. Você tinha que fazer logon em cada núcleo para administrar cada empresa ou organização.

O uso do gerenciamento de ocupantes simultaneamente ao Utilitário de serviços na nuvem da LANDesk reduz bastante a necessidade de múltiplos servidores núcleo. Depois de configurar o gerenciamento de ocupantes, os dispositivos configurados para ocupantes são exibidos em escopos separados do console. Você pode estar certo de quais artefatos dos ocupantes você está gerenciando enquanto você usa o console.

Cada ocupante que você cria recebe sua própria equipe de gerenciamento de usuário e escopo. Você pode designar usuários de console às equipes específicas de ocupantes e os escopos que eles devem administrar.

É possível que cada ocupante esteja associado á informações de contato, termos do contrato e rastreamento de uso da licença LANDesk.

Estes são os passos principais de configuração para o gerenciamento de ocupantes:

1. Na ferramenta de Gerenciamento de ocupantes, crie um ocupante.
2. Na ferramenta de Gerenciamento de usuários, adicione usuários de console a uma equipe ou escopo que possam ver o ocupante.
3. Na ferramenta de Configuração de agentes, crie uma configuração de agente, selecione o ocupante apropriado no painel de ocupantes e implante-o.
4. Use os grupos de ocupantes no console para gerenciar ocupantes.

Criando um ocupante

Use a ferramentas de Gerenciamento de ocupantes (**Ferramentas > Administração > Gerenciamento de ocupantes > Definição de novo ocupante**) para criar um ocupante. Você deve dar um nome e ID exclusivos ao ocupante. O nome de ocupante deve ser diferente que qualquer nome de escopo do RBA e de equipe existentes. A ID de ocupante só é editável quando o ocupante é criado.

Por padrão, a ID de ocupante é uma GUID, mas você pode substituí-la por qualquer combinação de letras (A-Z, a-z) números e traços. GUIDs podem ser difíceis de lembrar, portanto, considere usar algo como o número de cliente.

As informações restantes na caixa de diálogo **Configuração de ocupantes** são opcionais. Se você adicionar informações de contato, termos de contrato ou informações de licença, você pode boa parte destas informações em colunas na ferramenta de Gerenciamento de ocupantes.

As informações de licença são apenas informativas. O gerenciamento de ocupantes não limita o número de ocupantes ao número de **Licenças LANDesk designadas** inseridas. Rastrear licenças designadas pode ser útil para cobrança ou outros propósitos.

Use a guia **Notas** para adicionar todas as informações que desejar.

Ao criar um ocupante, uma equipe de gerenciamento de usuários e escopo são automaticamente criados com o mesmo nome do ocupante. Você deverá adicionar usuários de console que gerenciarão esse ocupante para a equipe de gerenciamento de usuário e escopo do ocupante. Somente os usuários de console que são membros da equipe de gerenciamento de usuários e escopo do ocupante poderão ver os grupos de ocupantes em várias partes do console.

Ao renomear um ocupante, o console renomeará automaticamente a equipe de gerenciamento de usuários e escopo associada e também renomeará todos os outros lugares no console onde o nome do ocupante aparece.

Criar um ocupante

Crie um ocupante se você quer compartimentar os dispositivos gerenciados por organização ou empresa.

Para criar um ocupante:

1. Clique em **Ferramentas > Administração > Gerenciamento de ocupantes**.
2. Digite um **Nome de ocupante** exclusivo.
3. Mude a **ID exclusiva** se você não quiser usar a GUID aleatória. Os caráteres válidos são A-Z, a-z, 0-9 e hifens.
4. Se quiser, entre dados adicionais relevantes ao ocupante.
5. Clique em **Salvar**.

Para adicionar usuários de console que gerenciarão o ocupante

1. Clique em **Ferramentas > Administração > Gerenciamento de usuários**.
2. Clique duas vezes na nova equipe nomeada de acordo com seu ocupante.
3. Selecione os usuários de console que gerenciarão dispositivos neste ocupante.
4. Clique em **OK**.

Para adicionar usuários de console ao escopo do ocupante

1. Clique em **Ferramentas > Administração > Gerenciamento de usuários**.
2. Clique com o botão direito no novo escopo que recebeu o mesmo nome do ocupante e clique em **Propriedades**.
3. Na página **Usuários e grupos**, selecione os usuários de console que gerenciarão os dispositivos neste ocupante.
4. Clique em **OK**.

Adição de dispositivos de ocupante

Depois de criar um ocupante, você pode adicionar dispositivos ao ocupante distribuindo uma configuração de agente atualizada que designa o ocupante para os dispositivos gerenciados do ocupante.

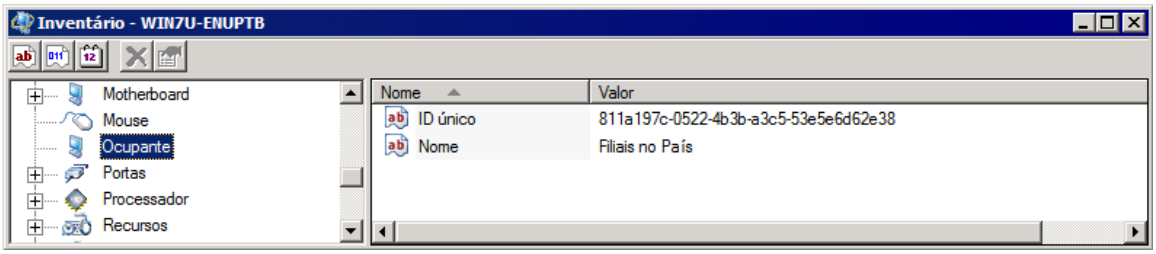
Cada ocupante que você cria tem seu próprio grupo de equipes na caixa de diálogo de configuração de agente. Use este grupo de equipes para organizar as configurações de agente de forma exclusiva para cada ocupante.

A caixa de diálogo Configuração de agente inclui uma página do **Ocupante** onde você pode selecionar o ocupante associado com uma configuração de agente.

Se você designar um ocupante a uma configuração de agente que não está no grupo de equipe do ocupante, a configuração não será automaticamente movida para o grupo de equipe do ocupante. Se você o quiser aí, mova ou copie-o manualmente.

Se você já distribuiu uma configuração de agente para dispositivos do ocupante, você não tem que redistribuir uma configuração de agente completa para atualizar as definições do ocupante em um dispositivo. Ao invés disso, após designar um ocupante na configuração de agente que você quer, use a botão da barra de ferramentas **Agendar atualização das configurações de agentes** na ferramenta de Configuração de agente para atualizar as configurações nos dispositivos-alvo.

A análise de inventário inclui a ID do ocupante encontrada na análise de inventário. Você pode ver o nome de ocupante e ID exclusiva sob o nó **Ocupante** na árvore de inventário do dispositivo.



Adição de dispositivos de ocupante

Adicione dispositivos a um ocupante designando um ocupante a uma configuração de agente e, sem seguida, distribuindo essa configuração de agente a dispositivos pertencendo ao ocupante.

Para adicionar dispositivos de ocupantes

1. Clique em **Ferramentas > Configuração > Configuração de agentes**.
2. Na árvore **Configuração de agente**, clique no grupo de configuração de agente que corresponde ao nome do ocupante. Se você quiser usar uma configuração de agente existente, copie e cole no grupo do ocupante.
3. Na caixa de diálogo **Configuração de agente**, certifique-se de selecionar **Designar um ocupante para esta configuração** e que você selecionou o ocupante que você quer definir para esta configuração de agente.
4. Clique em **Salvar**.
5. Se você está atualizando uma configuração de agente existente em dispositivos do ocupante, clique no botão da barra de ferramentas Agendar atualização das configurações de agentes. Caso contrário, distribua configuração do agente completa.
6. Adicione dispositivos pertencentes ao ocupante à tarefa agendada e agende sua execução.

Excluindo ocupantes e dispositivos de ocupante

Excluir um ocupante remove o grupo do ocupante das ferramentas de console relativas a ele. Ao excluir um ocupante será perguntado se você quer reatribuir as propriedades do objeto associados a ele (por ex., configurações do agente) a outro usuário de console. Caso você não faça isso, a propriedade do objeto órfão será revertida ao administrador da raiz do console.

A ID exclusiva do ocupante permanecerá nos dispositivos e não será removida quando você remover o ocupante. Se quiser, você pode remover a ID exclusiva de dispositivos de ocupante redistribuindo as definições das configurações de agente que não incluam um ocupante. Deixar a ID exclusiva nos ocupantes faz com que a análise de inventário preencha os dados de inventário da ID exclusiva, mas já que o dispositivo não terá um nome de ocupante associado com ele, o dispositivo não fará parte do grupo de equipes do ocupante.

Excluir um ocupante ou dispositivo de ocupante

Para excluir um ocupante

1. Clique em **Ferramentas > Administração > Gerenciamento de ocupantes**.
2. Selecione o ocupante que você quer excluir e pressione a tecla **Delete**.
3. Se quiser reatribuir objetos de ocupantes a um usuário de console ou equipe, outro que não o administrador da raiz, selecione o usuário ou equipe desejada.
4. Clique em **OK**.

Para remover um dispositivo de um ocupante

1. Na ferramenta Configuração de agente, selecione uma configuração de agente que não tem nenhum ocupante selecionado.
2. Clique no botão da barra de ferramentas Agendar atualização das configurações de agentes.
3. Adicione dispositivos que você quer remover dos ocupantes à tarefa agendada e programe sua execução.

Administrando dispositivos em um ocupante

Após a conclusão dos passos a seguir, você verá o ocupante como um item em várias partes do console:

1. Criar um ocupante
2. Atribua direitos de console para gerenciar este ocupante
3. Adicione dispositivos ao ocupante.

Você verá o ocupante em áreas como:

- Tela de rede, em **Dispositivos**, **Hosts SO virtuais**, **Consultas** e **Escopos**.
- Caixa de ferramentas de administração, em **Configuração do conjunto de colunas** e **Gerenciamento de usuários**.
- Caixa de ferramentas de distribuição, em **Métodos de entrega**, **Pacotes de distribuição** e **Gerenciar scripts**.
- Ferramenta gerenciamento de energia
- Caixa de ferramentas Segurança e conformidade, em **Patch e conformidade** e **Configurações de segurança**.

Você pode usar o grupo de equipes do ocupante nestas ferramentas para ver e gerenciar os dispositivos pertencentes a um ocupante. Somente usuários de console com direitos para gerenciar de um ocupante poderá ver este ocupante no console.

Uma maneira fácil de selecionar dispositivos de ocupante em uma tarefa agendada é usar o mouse para arrastar o escopo do ocupante **Tela de rede** e soltar na tarefa desejada.

NOTA: Para dispositivos do Windows a ID exclusiva do ocupante é adicionada ao registro:

HKLM\SOFTWARE\LANDesk\ManagementSuite\WincClient\Tenant\TenantUID

Em dispositivos Macintosh a ID exclusiva do ocupante é adicionada a uma plist:

/Library/Preferences/com.landesk.ldms.plist

Virtualização de aplicativos

LANDesk Application Virtualization

O LANDesk Application Virtualization é um suplemento LANDesk Management Suite vendido separadamente pela LANDesk Software, Inc.. O LANDesk Application Virtualization usa a tecnologia Thinstall para virtualizar um aplicativo, armazenando-o em único executável independente que contém o aplicativo e as dependências de .DLL/driver de dispositivos.

Os aplicativos virtualizados são executados em um ambiente isolado sem alterar a instalação do Windows. Eles podem até mesmo serem executados em dispositivos bloqueados sem a necessidade de privilégios adicionais.

Para mais informações, consulte a documentação que acompanha à LANDesk Application Virtualization. Ao usar a LANDesk Application Virtualization com o Management Suite, você poderá distribuir e gerenciar aplicativos virtualizados.

NOTA: Uso de versões não-LANDesk de Thinstall
A versão LANDesk de Aplicativos virtualizados da Thinstall possui personalizações específicas ao Management Suite. Outras versões dos aplicativos virtualizados da Thinstall podem não funcionar corretamente com a monitoração de licenças de software ou com o analisador de inventário.

Distribuir um aplicativo virtualizado

Geralmente, os aplicativos virtualizados consistem em um ou mais arquivos executáveis. Você pode usar a distribuição de software para implantar esses executáveis de aplicativos virtualizados em dispositivos gerenciados. Também é possível utilizar quaisquer um dos métodos de entrega para distribuição de software com pacotes de aplicativos virtualizados, incluindo a execução da origem. Quando você distribui um pacote de aplicativo virtualizado para execução da origem, os dispositivos gerenciados usam um ícone de atalho do aplicativo para sua execução pela rede.

Para criar um pacote de aplicativo virtualizado

1. Use o LANDesk Application Virtualization para criar o executável do aplicativo virtualizado.
2. Clique em **Ferramentas > Distribuição > Pacotes de distribuição**.
3. No menu de atalhos do grupo de pacotes desejado, clique em **Novo pacote de distribuição > Novo pacote de aplicativo virtualizado**.
4. Na caixa de diálogo **Pacote de distribuição**, insira as informações do pacote e altere as opções que desejar. Observe que é necessário inserir o nome do pacote, a descrição e o arquivo primário. Para obter mais informações sobre cada página, clique em **Ajuda**.
5. A página **Atalho** é a única página específica para aplicativos virtualizados. Insira o ícone de atalho em **Nome**. Você também pode especificar se deseja que o ícone seja inserido na **Área de trabalho** e/ou no **menu Iniciar**. Se você selecionar o menu Iniciar, será possível também inserir o **Nome da pasta programas** que conterá o atalho. O caminho da pasta inserido será exibido em **Todos os programas**.
6. Clique em **OK** quando tiver concluído. O seu script será exibido sob o item da árvore para o tipo de pacote e o proprietário selecionados.

Quando você distribuir um aplicativo virtualizado, a distribuição de software copiará os executáveis para esta pasta nos dispositivos gerenciados.

- %programfiles%\LANDesk\VirtualApplications\<caminho de origem da distribuição>.

O caminho completo do aplicativo virtualizado inclui o caminho de origem da distribuição do software para ajudar a impedir problemas com nomes de arquivos duplicados. Por exemplo, se o seu caminho de distribuição for vapps\myapp.exe, o caminho nos dispositivos gerenciados será %programfiles%\LANDesk\VirtualApplications\vapps\myapp.exe.

Você poderá alterar o caminho padrão de aplicativos virtualizados na página **Distribuição de software** da caixa de diálogo **Configuração de agentes**.

Alguns aplicativos virtualizados necessitam de vários executáveis. Se este for o caso, você poderá criar um pacote de distribuição separado para esses executáveis de aplicativos virtualizados adicionais. Em seguida, quando você criar um pacote de distribuição para o executável de aplicativo virtualizado principal, será possível incluir pacotes executáveis adicionais dependentes. Dessa forma, se os executáveis dependentes ainda não estiverem lá, eles serão instalados automaticamente.

Os executáveis dependentes precisarão estar na mesma pasta compartilhada quando os pacotes de distribuição forem criados. Isso garantirá que os pacotes dependentes sejam distribuídos para a mesma pasta do dispositivo gerenciado. Se os executáveis dependentes não estiverem na mesma pasta do dispositivo gerenciado, eles não serão executados.

Na primeira vez em que alguém executa um aplicativo virtualizado em um dispositivo, a caixa de diálogo "Contrato de licença de tempo de execução da Thinstall" é exibida. É necessário que os usuários cliquem em **Continuar** para executar o aplicativo virtualizado. Isso só é necessário uma vez.

Área de segurança do aplicativo virtual

Por padrão, os aplicativos virtualizados criam arquivos temporários necessários para que sejam executados nesta pasta:

- Documents and Settings\<nomeusuário>\Application Data\Thinstall\

O analisador de inventário não analisa essa pasta para impedir relatos falsos de aplicativos no sistema.

Uso do monitoramento do inventário e das licenças de software com aplicativos virtualizados

Os executáveis de aplicativos virtualizados criados com LANDesk Application Virtualization possuem informações de propriedades adicionais que ajudam a Management Suite no monitoramento do inventário e das licenças de software. No Windows Explorer, se você clicar com o botão direito do mouse em um executável de aplicativo virtualizado e clicar em **Propriedades**, as informações de versão adicionais serão exibidas:

- **ThinstallLicense:** O tipo de licença e endereço de e-mail de assinatura do LANDesk Application Virtualization.
- **ThinstallVersion:** A versão do empacotador LANDesk Application Virtualization usada para criar este pacote.

Você pode usar essas informações nas suas consultas de inventário para localizar aplicativos virtualizados que foram analisados pelo analisador de inventário. Geralmente, as propriedades do executável do aplicativo virtualizado correspondem às propriedades do executável principal dentro do aplicativo virtualizado. Na tela de inventário para um dispositivo, os aplicativos virtualizados são exibidos na lista **Software > Pacote**. Os aplicativos virtualizados na lista possuem o valor "Sim" no atributo "Aplicativo virtual".

Entretanto, alguns aplicativos não fornecem informações de versão antes que sejam virtualizados. Nesse caso, eles não serão exibidos como aplicativos virtualizados no inventário, apesar de serem virtualizados.

Os executáveis de aplicativos virtualizados serão analisados automaticamente pelo analisador de inventário somente se você estiver usando a análise de inventário MODE=ALL. Se você não estiver usando MODE=ALL e desejar obter informações de inventário de aplicativos virtualizados no banco de dados, será necessário adicionar as informações de executáveis de aplicativos virtualizados à monitoração de licenças de software **Inventário > Arquivos > lista A serem analisados**. O analisador de inventário somente verifica o executável do aplicativo virtualizado. Ela não analisa dentro do executável.

A monitoração de licenças de software descobrirá automaticamente aplicativos virtualizados e os incluirá na lista **Definições de produto > Descobertos automaticamente**. A descoberta automática de aplicativos pela monitoração de licenças de software não utiliza o analisador de inventário. A monitoração de licenças de software detecta o menu Iniciar ou o atalho do desktop para o aplicativo.

Um aplicativo virtualizado descoberto na lista **Descobertos automaticamente** possuirá somente o único executável de aplicativo virtualizado na sua lista de arquivos, mas a definição do produto ainda será baseada no produto dentro do executável do aplicativo virtualizado. A monitoração de licenças de software não procura dentro do executável do aplicativo virtualizado. Portanto, ela não pode incluir outros arquivos que normalmente seriam atribuídos a um produto quando ele fosse instalado sem virtualização.

Web console

Sobre o Web Console

OManagement Suite console Web permite que você automatize as tarefas de gerenciamento de sistemas e computadores de mesa, servidores de controle e dispositivos móveis. Ela difere do Console de gerenciamento da LANDesk porque pode ser acessada através de um navegador, e não como um executável do Windows.

O Web console usa a infra-estrutura da rede existente para estabelecer conexões com os dispositivos que ele gerencia. Isso simplifica tremendamente a tarefa de gerenciar a rede existente, seja o gerenciamento de uma pequena rede ou de um grande ambiente empresarial, mesmo quando não você não estiver na sua mesa.

O Web console executa no computador baseado em Windows usando os navegadores e plugins abaixo:

- Internet Explorer 8 ou superior
- Mozilla Firefox 4.0 ou posterior
- Google Chrome
- Adobe Flash Player 9 ou posterior

Como iniciar o Web console

Para iniciar o console Web

1. Em um computador da rede, abra um navegador.
2. No campo de endereço do navegador, insira uma URL que aponte para o servidor núcleo, seguido por **/remote** (no formato http://<webservername>/remote).
3. Se aparecer uma caixa de diálogo de login, digite seu nome de usuário e senha do Windows relativos ao núcleo ao qual você está se conectando e clique em **OK**.
4. Após a autenticação, aparecerão links no painel esquerdo de navegação relativos às tarefas que você tem direito de executar, por exemplo, criação de consultas, controle remoto de clientes, distribuição de software e exibição de relatórios.

Clique aqui para uma descrição da caixa de diálogo de início de sessão

Use esse diálogo para iniciar o console e conectar-se a um servidor núcleo.

- **Nome de usuário:** identifica um usuário. Esse usuário pode ser um administrador ou outro tipo de produto com acesso restrito. O usuário deve ser um membro do grupo LANDesk Management Suite no servidor núcleo. Se estiver se conectando a um servidor núcleo remoto, digite o nome de domínio e o nome do usuário.
- **Senha:** a senha do usuário.

Identificação e solução de problemas

- Se a lista de dispositivos e os botões não aparecerem quando o console for iniciado, pode ser necessário ativar o servidor núcleo.
- Se você não sabe a URL das páginas console Web, contacte a pessoa que instalou o console Web, muito provavelmente o administrador de rede para o seu site.

- Se você não consegue ver alguns dos links do espelho esquerdo de navegação, o administrador de rede é mais provável comManagement Suite administração baseada em papel ou função opção de nível de segurança que limita a realização de determinadas tarefas que você tem os direitos para fazer.

Usar o Web Console

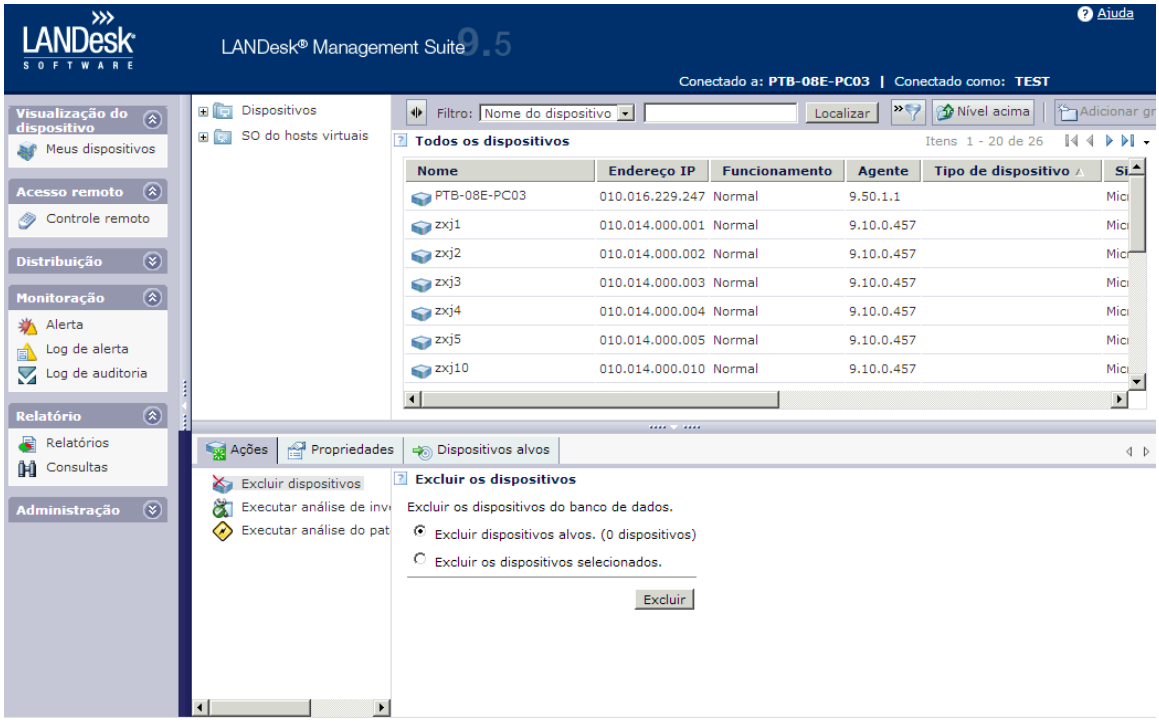
Este tópico descreve oManagement Suite console Web e como utilizar-lo.

Lembre-se de que se você não ver uma ferramenta, você provavelmente não tem direitos para a ver. Estes direitos são determinados pelos direitos de acesso e alcance do dispositivo atribuído a você pelo administradorManagement Suite.

Layout do console Web:

O console Web tem quatro áreas principais que você interaja com:

- A barra de título
- A Caixa de ferramentas
- O painel de ferramentas
- O painel de ações



A **barra de título** exibe o dispositivo que você está conectado e o usuário que está logado como. Ela inclui um link de ajuda que abre tópicos de ajuda para o console Web.

O **toolbox** mostra ferramentas disponíveis, agrupados em capítulos. Clique nas setas ao lado de uma rubrica para expandir ou fechar o grupo.

No lado direito do console existem vários conteúdos variáveis em função da ferramenta em uso. Se esta área é dividida, a parte superior é referido como o **painel do aparelho e a** parte inferior do painel da **ação** . O painel de ferramentas mostra os elementos básicos da ferramenta que você selecionou, e tipicamente no painel de ação que você irá selecionar as ações ou exibir os resultados da tarefa que você está fazendo.

Você pode redimensionar os painéis e colunas do console Web. Você também pode ampliar ou reduzir o tamanho dos elementos ferramentas para que você possa visualizá-las melhor.

NOTA: Para que as caixas de diálogos e as janelas sejam mostradas corretamente na tela, o site do Management Suite deverá ser adicionado à lista de permissões do bloqueador de popup do navegador.

Continue lendo este tópico para obter informações sobre:

- Lista Meus dispositivos
- Ícones de dispositivos
- Uso dos menus de atalho
- Uso das ferramentas
- Exibindo propriedades do dispositivo

Lista Meus dispositivos

A **minha lista de dispositivos** é a janela principal, que é exibido quando você iniciar o console Web e é o ponto de partida da maioria das ferramentas. Ela contém os grupos e sub-grupos seguintes. Além disso, dependendo dos seus direitos de acesso e do escopo dos dispositivos, você pode criar seus próprios grupos para facilitar o gerenciamento dos dispositivos.

Algumas comumente ações usadas nesta lista incluem o seguinte:

- Clique com o botão direito na lista **Dispositivos** para ver as opções disponíveis do dispositivo como, por exemplo, Ping, Controle remoto e Alvo.
- Para selecionar várias entradas da lista, clique no primeiro item, pressione e segure a tecla **Shift** e, em seguida, clique no último item.
- Para selecionar várias entradas não consecutivas da lista, clique no primeiro item, pressione e segure a tecla **Ctrl** e, em seguida, clique em cada item.
- Clique duas vezes em um dispositivo na lista **Todos os dispositivos** para abrir uma janela de inventário inteiro de dispositivos que mostra todas as informações do dispositivo.

Todos os dispositivos

A lista **Todos os dispositivos** relaciona os dispositivos do usuário atualmente conectado, com base em seu escopo, em uma lista sem subgrupos. Quando conectado a um determinado servidor núcleo, o administrador pode ver todo dispositivo gerenciado por esse servidor núcleo. Os usuários dos produtos, por outro lado, são restritos e podem ver apenas os dispositivos contidos no seu escopo atribuído (um escopo é baseado em uma consulta do banco de dados ou em um local de diretório).

Os dispositivos com agentes (de gerenciamento padrão e inventário) são exibidos automaticamente na lista **Todos os dispositivos** quando forem analisados e inseridos são analisados e colocados no banco de dados núcleo pelo analisador de inventário. Normalmente, essa análise é feita pela primeira vez durante a configuração inicial do dispositivo. Após um dispositivo ser analisado e colocado no banco de dados núcleo, ele se torna um dispositivo gerenciado—podendo então ser gerenciado pelo servidor núcleo.

Pelo fato de o grupo **Todos os dispositivos** ser preenchido automaticamente por meio de uma análise de inventário, talvez não seja preciso descobrir dispositivos manualmente. Entretanto, para descobrir dispositivos que ainda não estão no banco de dados núcleo (ou para mover dispositivos não gerenciados para um grupo de dispositivos), você pode usar a ferramenta Descobrir dispositivos para fazer uma análise da rede e encontrar dispositivos.

O grupo **Todos os dispositivos** fornece as seguintes informações de cada dispositivo. Para classificar uma coluna, clique no seu cabeçalho, para reverter a classificação, clique no cabeçalho novamente. Clique duas vezes em **Todos os dispositivos** para abrir a lista.

- **Nome:** o nome do dispositivo host, por exemplo, o nome do computador no Windows.
- **Endereço IP:** o endereço IP do dispositivo.
- **Funcionamento:** o status de funcionamento e a disponibilidade do dispositivo. Os estados podem ser: Normal, Aviso, ou Crítico.
- **Agente:** o agente atualmente em execução no dispositivo.
- **Tipo de dispositivo:** mostra o tipo de hardware no computador (Intel AMT, IPMI, ASIC ou IPMI Avançado).
- **Sistema operacional:** o tipo de sistema operacional em execução no dispositivo.
- **Em funcionamento desde:** a data e o horário desde o ínicio da operação contínua do dispositivo (no fuso horário do banco de dados).
- **LaunchPad:** [MAIS INFO]

Quando não há nenhum agente instalado em um dispositivo, as colunas Nome e Endereço IP são as únicas que contêm informações. Em alguns casos, o sistema operacional também é exibido.

Quando você seleciona um dispositivo, as propriedades do dispositivo são mostradas no painel **Propriedades**, abaixo da lista de dispositivos. O **painel Propriedades** mostra dispositivo básico atributos:

- **ID:** o número de identificação do dispositivo. Este número é determinado pela seqüência em que o dispositivo foi adicionado à **lista de todos os dispositivos**.
- **Endereço IP:** o endereço IP do dispositivo.
- **Fabricante:** o fabricante do dispositivo.
- **Modelo:** O modelo do dispositivo.
- **Velocidade do processador:** a velocidade da CPU do dispositivo.
- **Tipo de processador:** o tipo da CPU do dispositivo.

Para mais ações disponíveis no painel de propriedades, consulte "Sobre a guia Propriedades" na página 893 .

Meus dispositivos

A lista **Meus dispositivos** mostra grupos de dispositivos criados pelo usuário atualmente conectado. Os grupos Meus dispositivos não são visíveis aos usuários e não podem ser usados por eles.

Dispositivos públicos

A lista **Dispositivos públicos** mostra grupos de dispositivos que foram criados por um usuário com direitos de Administrador. Esses grupos são visíveis aos outros usuários.

Hosts de SO virtuais

A lista de **Hosts de SO virtuais** mostra os servidores VMware ESX configurados como hosts virtuais descobertos pela seleção da opção Hosts virtuais na configuração na descoberta de dispositivo. Ao clicar em **Hosts de SO Virtuais** ou em sub-grupos na tela de árvore, os hosts são mostrados como nós de extremidade na janela do dispositivo. Ao clicar no nome do host na tela de árvore, o host é um contêiner e as máquinas virtuais em execução nele são exibidas na lista de dispositivo.

Ícones de dispositivos

Os ícones de dispositivo na lista todos **os dispositivos** apresentam o estado atual de saúde de cada dispositivo, se o dispositivo inclui um agente com o **tempo real inventário e monitoramento** opção selecionada. Você pode atualizar o estado de funcionamento dos dispositivos, um de cada vez, ao selecioná-los na lista **Meus dispositivos** e clicar no botão da barra de ferramentas **Atualizar**.

Existem quatro ícones de status:

Ícone	Descrição
	Dispositivo com o estado Normal
	Dispositivo com o estado Aviso
	Dispositivo com o estado Crítico
	Dispositivo com o estado Desconhecido

NOTA: Estes ícones requerem pelo menos um 16-bit color-ajuste de profundidade para exibir corretamente. Se os ícones parecerem fora de foco no seu console, mude suas configurações de cores em Propriedades de exibição do Windows.

Uso dos menus de atalho

Menus de atalho (contexto) estão disponíveis para todos os itens do console, inclusive grupos, dispositivos, consultas, tarefas agendadas, scripts, etc. Os menus de atalho proporcionam acesso rápido às tarefas comuns e às informações críticas de um item.

Para ver o menu de atalho de um item, clique nele com o botão direito. Por exemplo, quando você clicar com o botão direito em um dispositivo gerenciado na lista **Meus dispositivos**, o seu menu de atalho geralmente mostrará as seguintes opções:

- **Remover do grupo:** remove o item de um grupo definido pelo usuário.
- **Alvo:** transfere o dispositivo selecionado para a lista Dispositivos alvo. (Se os dispositivos alvo não aparecerem na Lista de alvos, clique em **Atualizar** na guia **Dispositivos alvo**.)
- **Fazer ping ao dispositivo:** verifica se o dispositivo está respondendo.
- **Fazer tracert para o dispositivo:** envia um comando de rastreamento de rota para ver um pacote de rede ser enviado e recebido e o número de saltos necessários para o pacote chegar ao destino.
- **Analisar dispositivo:** analisa o dispositivo para verificar vulnerabilidades. Clique em **Iniciar análise**.

- **Launch DSView**: Abre o add-on Avocent DSView, se instalado.
- **Controle remoto:** Inicia a janela do controle remoto, permitindo o acesso direto ao dispositivo selecionado no console.

A ajuda não abrange os menus de atalho de cada item do console, mas recomendamos que você clique com o botão direito do mouse em qualquer item para ver as opções disponíveis.

Uso das ferramentas

As ferramentas são agrupadas na caixa de ferramentas em seções, com cabeçalhos como **Tela de dispositivo** e **Acesso remoto**. Clique nas setas ao lado de uma rubrica para expandir ou fechar o grupo.

O administrador vê todas as ferramentas da Caixa de ferramentas. Os outros usuários podem ver apenas as ferramentas (os recursos) permitidas pelos seus direitos atribuídos. Por exemplo, se um usuário não tem o direito de relatórios, a ferramenta **de Relatórios** não aparecem na caixa de ferramentas.

A seguir, é apresentada uma lista completa das ferramentas:

- Meus dispositivos:
- **Controle remoto:** Controlar remotamente dispositivos e arquivos de troca com eles.
- **Avocent DSView:** mostra uma lista de dispositivos com o Avocent DSView. Clique com o botão direito em um dispositivo na lista para iniciar a sessão do DSView.
- **Distribuição:** distribui pacotes de software, utiliza scripts personalizados, agenda distribuições e cria tarefas de distribuição de software.
- **Gerenciador do link do LaunchPad:** Torna disponível links de pacote de software aos usuários com LANDesk LaunchPad.
- **Scripts:** Criar e gerenciar os scripts.
- **Gerenciador de diretórios:** permite localizar, acessar e gerenciar dispositivos em outros diretórios via LDAP (Lightweight Directory Access Protocol).
- **Tarefas agendadas:** permite ver todas as tarefas que estão atualmente agendadas ou concluídas.
- Alertas:
- Log de alerta:
- **Relatórios:** gerencia relatórios de serviço pré-definidos.
- **Consultas:** cria e modifica consultas no banco de dados para isolar dispositivos específicos que satisfaçam critérios determinados.
- **Preferências:** permite criar atributos de inventário personalizados e ver informações sobre o licenciamento.

Ver propriedades do dispositivo e inventário

Na tela **Meus dispositivos,** você pode exibir informações sobre um dispositivo rapidamente, basta clicar com o botão direito do mouse no dispositivo e selecionando **Propriedades** no painel de ações.

Veja outras informações mais detalhadas sobre o dispositivo em seus dados de inventário. Veja todos os dados do inventário da tela **Todos os dispositivos** com um clique duplo no dispositivo, ou selecionando a guia **Exibir inventário** no painel **Propriedades** para abrir a janela inteira do **Inventário**.

Sobre a guia Propriedades

Use a guia Propriedades para exibir informações úteis sobre o dispositivo selecionado. A tela inclui um resumo rápido das propriedades e os seguintes botões:

- **Visualizar inventário:** Clique neste botão para abrir o inventário completo do dispositivo selecionado em uma tela de árvore. Esses dados são coletados pelo analisador de inventário e armazenados no banco de dados. O modo de exibição detalhado apresenta todos os possíveis itens de inventário disponíveis para um dispositivo, para alguns itens (que não estão habilitados para o dispositivo selecionado) não terá nenhum dados. Clique em um item na tela para exibir detalhes sobre ele nesse dispositivo específico. Para voltar para o modo de visualização predefinido, clique no nome do dispositivo, a raiz de a vista
- **Controle remoto:** Inicia a janela do controle remoto, permitindo o acesso direto ao dispositivo selecionado no console.
- **SSH:** Fornece acesso seguro ao dispositivo Linux selecionado. Se o dispositivo selecionado não for Linux, esta opção estará esmaecida.
- **SFTP:** Fornece acesso FTP seguro ao dispositivo Linux selecionado. Se o dispositivo selecionado não for Linux, esta opção estará esmaecida.

Dispositivos alvo [console Web]

A lista **Dispositivos alvo** o habilita a completar numerosas tarefas em dispositivos selecionados como, por exemplo, distribuir agentes ou fazer análise para encontrar atualizações de software para um grupo selecionado de dispositivos.

O número recomendado de dispositivos que você deve adicionar à lista é 250 ou menos. Os dispositivos permanecerão na lista até ser atingido o limite de tempo ou o término de sua sessão do Console (após 20 minutos de inatividade).

Você pode tornar dispositivos alvos selecionando-os de qualquer lista de dispositivos. Se o dispositivo que deseja não aparece na lista, use o botão **Localizar** na barra de ferramentas. Procure um dispositivo específico ou vários clientes usando os caracteres curinga % ou *.

Se houver um ou mais dispositivos na lista **Dispositivos alvo**, você pode executar tarefas como, distribuição de uma configuração de agente para cada dispositivo alvo.

Dispositivos de destino usando o console Web

1. Na lista **Meus dispositivos** ou na lista **Todos os dispositivos**, clique no dispositivo que deseja selecionar como alvo para uma ação. Selecione vários dispositivos utilizando+clique ou Ctrl+clique Shift.
2. Clique no botão **Alvo**. Se não estiver visível, clique no botão **Filtro** na barra de ferramentas para esconder as opções de filtro (o botão de destino está na extrema direita).

Os dispositivos estão relacionados no painel de ação na guia **Dispositivos-alvo.** Quando eles são mostrados nessa guia, você pode abrir uma ferramenta (por exemplo, Distribuição) e agendar uma tarefa, a qual pode ser aplicada aos dispositivos alvo.

NOTA: As listas de dispositivos se estendem por várias páginas e quando você selecione dispositivos é necessário clicar no botão **Alvo** para cada página. Você não pode selecionar dispositivos em várias

páginas e clicar nos botões apenas uma vez para todas as páginas.

NOTA: Clique na seta para baixo, na parte inferior da barra de ferramentas, do lado direito, para definir quantos dispositivos quer mostrar por página. É possível mostrar até 500 dispositivos por página. Para alterar permanentemente o número de dispositivos apresentados na lista de dispositivos, clique em **Administração > Preferências > Configurações de página** .

Filtrando a lista de exibição [console Web]

As listas **de dispositivos têm** uma opção de filtro que você pode usar para determinar quais dispositivos aparecem na lista. Você pode filtrar por um dos quatro tipos de critérios (nome do dispositivo, endereço IP, sistema operacional ou nome de login). Use um caractere curinga (% ou *) para selecionar uma faixa de itens com um identificador semelhante.

Para filtrar a lista de servidores

1. Clique em **Os meus dispositivos** e navegar para um grupo de **dispositivos** .
2. Se as **opções do filtro** não são visíveis, clique no **botão Filtro** na barra de ferramentas.
3. Na lista Filtro, selecione o **nome do dispositivo** e **endereço IP**, **sistema operacional** , ou nome **de login** .
4. Configurar os parâmetros do filtro, digitando na caixa de texto.

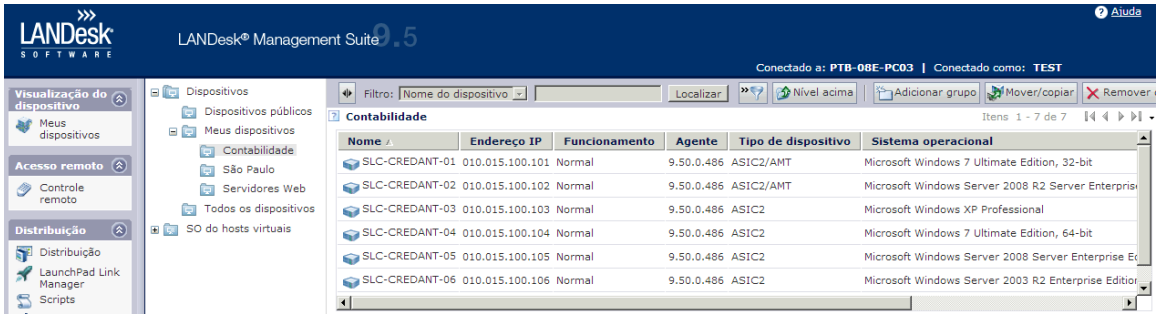
   Nesta casa, os caracteres estendidos abaixo não são suportados:

   Por exemplo, se você fez um filtro por nome do dispositivo, digite o nome do host ou uma faixa de nomes de computadores. Pode introduzir caracteres curinga para encontrar alguns nomes (como * srv)de computador .
5. Clique em **Localizar**.

Uso de grupos [console Web]

Você pode organizar os dispositivos em grupos para facilitar o gerenciamento. Você pode criar grupos para organizar dispositivos de acordo com sua função, localização geográfica, departamento, atributos de dispositivo ou qualquer outra categoria que atenda às suas necessidades. Por exemplo, você pode criar um grupo de servidores web para todos os servidores configurados como servidores web ou um grupo que inclua todos os dispositivos executando um SO específico.

Os detalhes do monitor abaixo exibem três grupos de dispositivos criados pelo usuário atual.



Clique com o botão direito em um grupo para abrir, excluir ou alvo todos os dispositivos que contém para ações como distribuição de software ou agente implantação.

A tela principal **Dispositivos** contém os seguintes grupos:

- **Meus dispositivos:** Relaciona os grupos/dispositivos do usuário atualmente conectado, de acordo com o escopo desse usuário. O usuário pode criar subgrupos de dispositivos apenas em **Meus dispositivos**. Os usuários podem adicionar dispositivos no seu grupo **Meus dispositivos** ou em qualquer um dos seus subgrupos transferindo ou copiando os grupos **Dispositivos públicos** e **Todos os dispositivos**. Todos os usuários podem criar grupos em **Meus dispositivos** no console do Windows.
- **Dispositivos públicos:** Relaciona os grupos/dispositivos que o administrador adicionou do grupo **Todos os dispositivos**. O administrador (usuário com direitos de Administrador) pode ver todos os dispositivos desse grupo, ao passo que os outros usuários podem ver apenas os dispositivos permitidos pelo seu escopo. Apenas os administradores podem criar grupos em **Dispositivos públicos**.
- **Todos os dispositivos:** Relaciona todos os dispositivos que podem ser vistos pelo usuário atualmente conectado, com base em seu escopo, em uma lista sem subgrupos. Para o administrador, **Todos os dispositivos** relaciona todos os dispositivos que foram analisados ou movidos para o banco de dados núcleo. Os dispositivos configurados com o agente padrão são exibidos automaticamente no grupo **Todos os dispositivos** quando são analisados e colocados no banco de dados núcleo pelo analisador de inventário. Os usuários, inclusive os administradores, não podem criar grupos em **Todos os dispositivos**.

Criação de um grupo de dispositivos [console Web]

Grupos ajudam a organizar dispositivos na lista **Dispositivos** do console. Você pode criar grupos para organizar dispositivos de acordo com sua função, localização geográfica, departamento, atributos ou qualquer outra categoria que atenda às suas necessidades. Por exemplo, você pode criar um grupo de marketing para todos os dispositivos do departamento de marketing ou um grupo que inclua todos os dispositivos que utilizam um SO específico. É possível criar grupos dentro de grupos, por exemplo, todos os dispositivos executando determinado SO em determinada localização.

Os grupos são organizados como se segue:

- **Dispositivos**: Para criar grupos em **Dispositivos**, primeiro é preciso selecionar **Meus dispositivos** ou **Dispositivos públicos**.
- **Meus dispositivos:** Meus dispositivos só podem ser vistos pelo usuário que os criou.
- **Dispositivos públicos:** Somente os administradores podem criar ou modificar grupos nos **Dispositivos públicos**, mas qualquer um pode ver os grupos.
- **Todos os dispositivos:** Não há nenhum subgrupo em **Todos os dispositivos**.

Para criar um grupo

1. Na lista **de dispositivos**, clique em meus **aparelhos ou dispositivos públicos** .
2. Clique no botão **Adicionar grupo** na barra de ferramentas.
3. Digite um nome para o novo grupo e clique em **OK**.

Para excluir um grupo

1. Na tela de dispositivo do console, clique no pai do grupo que deseja excluir.
2. No painel de ferramentas, clique com o botão direito do mouse sobre o grupo que você deseja excluir e clique em **Excluir grupo**.

Usar a guia Ações [console Web]

Use a guia **Ações** para executar as seguintes operações nos dispositivos selecionados específicos:

- Excluir dispositivos do banco de dados.
- Executar análise de inventário em dispositivos selecionados
- Execute as análises de patch e conformidade em dispositivos selecionados

Para excluir dispositivos do banco de dados

Pode selecionar os dispositivos da lista atual do dispositivo, ou alvo uma lista de dispositivos (que é útil quando existem várias páginas na lista de dispositivos).

1. No console Web, clique em **Meus dispositivos** e selecione ou alvo os dispositivos para eliminar.
2. Clique na guia **Ações** > **Excluir dispositivos**. Selecione Excluir **orientadas ou dispositivos dispositivos selecionados de riscar o que não interessa**.
3. Clique em **Excluir** para confirmar que você quer excluir os dispositivos.

A função de excluir pode eliminar dispositivos únicos ou múltiplos de qualquer grupo de padrão ou grupo criado pelo usuário. Quando o dispositivo é excluído de um grupo, ele é completamente removido de todas as listas de dispositivos gerenciados/inventariados, inclusive do grupo padrão **Todos os dispositivos**.

Para executar um análise de inventário em dispositivos selecionados

Pode selecionar os dispositivos da lista atual do dispositivo, ou alvo uma lista de dispositivos (que é útil quando existem várias páginas na lista de dispositivos).

1. No console Web, clique em **Meus dispositivos** e selecione ou alvo os dispositivos para eliminar.
2. Clique na guia **Ações** > **Executar análise de inventário**. Selecione **Analisar dispositivos-alvo** ou **Analisar dispositivos selecionados,** como desejar.
3. Selecione o tipo de digitalização (apenas o Hardware, Hardware e software, ou Sincronização completa).
4. Clique em **Analisar** .

As notas do Estado sobre o andamento do processo de digitalização são exibidos no painel da ação.

Para executar uma Análise de patch e conformidade em dispositivos selecionados

Pode selecionar os dispositivos da lista atual do dispositivo, ou alvo uma lista de dispositivos (que é útil quando existem várias páginas na lista de dispositivos).

1. No console Web, clique em **Meus dispositivos** e selecione ou alvo os dispositivos para eliminar.
2. Clique na guia **Ações** > **Executar análise de patch e conformidade**. Selecione **Analisar dispositivos-alvo** ou **Analisar dispositivos selecionados,** como desejar.
3. Selecione o tipo de análise (análise de patch e conformidade, análise de conformidade).
4. Clique em **Analisar** .

Alterar configurações da página [console Web]

Utilize **Configurações de página para** definir preferências de exibição de páginas listando os dispositivos ou exibição de gráficos. Isso não inclui o dashboard funcionamento, que contém caixas de diálogo separadas para a definição das preferências de exibição.

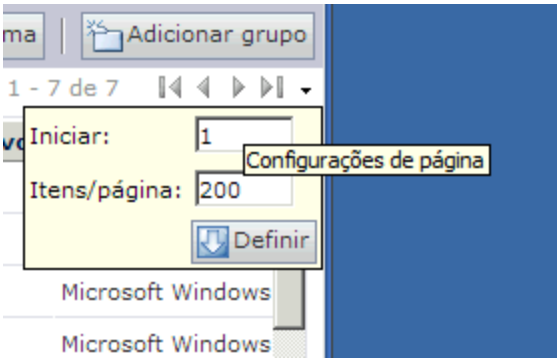
Para alterar as configurações de página do console Web

1. Na caixa de ferramentas do console Web, clique em **Administração > Preferências**.
2. Clique na guia **Configurações de página**.
3. Na lista **Tipo de gráfico**, selecione o tipo de imagem que desejar exibir e clique em **Relatórios**.
4. No campo **Itens/página**, digite o número máximo de itens que você deseja exibir em cada página que usar paginação (o valor máximo permitido é 500).
5. Para mostrar o texto ao lado dos botões nas barras de ferramentas, selecione **Mostrar texto nas barras de ferramentas**.
6. Para garantir que a sessão da Web que você está executando para ver o console Web não tempo, selecione **Sempre manter a sessão Web ativada**.
7. Clique em **Atualizar**.

NOTA: Você pode exibir texto ao lado dos botões nas barras de ferramentas para ajudar os novos usuários a identificarem os recursos. Se esta opção não for selecionada, apenas os ícones aparecerão nas barras de ferramentas. Entretanto, os ícones mostram texto quando o ponteiro do mouse é passado sobre eles.

Para exibir mais dispositivos durante a visualização de uma lista

1. Ao ver a lista de dispositivos, clique na seta para baixo no extremo direito (sob a barra de ferramentas) para abrir a **página de Definições** caixa.



2. Digite um número na**/página de itens** box (máximo 500).
3. Para começar a lista mais tarde do que o primeiro registro, altere o número na caixa de **iniciar**.
4. Clique em **Configurar**.

As alterações só são válidos enquanto estiver a trabalhar na lista atual. Se você mudar para outra lista de dispositivos, o número de dispositivos exibidos reverte para a definição de efeito sobre o **guia de configurações de página**.

Configuração de colunas personalizadas [console Web]

Use **Colunas personalizadas** para modificar nomes e campos de colunas. As mudança que você fizer nas colunas não serão vistas por outros usuários. As alterações personalizadas da coluna aparecem na tela **Meus dispositivos**.

O console Web inclui uma coluna de padrão definido com oito colunas. Não é possível editar o conjunto padrão, mas você pode definir um conjunto de colunas personalizadas para usar como padrão.

NOTA: Não é recomendável criar colunas personalizadas nas quais possa haver múltiplos nomes de campo. Por exemplo, se você criar um computador.Software.pacote.campo de nome e um dispositivo tinha vários pacotes instalados, Management Suiteirá listar apenas um nome de pacote por linha, mesmo se os diferentes nomes de pacotes estão no mesmo dispositivo. Nesta situação, a **lista de todos os dispositivos irão** mostrar várias entradas para o mesmo dispositivo.

Para criar um conjunto de colunas personalizadas

1. Na caixa de ferramentas do console Web, clique em **Administração > Preferências**.
2. Clique na guia **Colunas personalizadas** > **Novo .**
3. Digite um nome para o conjunto de colunas.
4. Na caixa superior, navegar pelas pastas para encontrar o atributo que deseja para cada cabeçalho de coluna. Selecione um atributo e clique em **Adicionar** .

   A caixa contém uma estrutura de pastas, começando com **Computador** , que representa todos os dados de inventário que está atualmente na banco de dados. Os atributos individuais têm um ícone de atributo .

   NOTA: Se você selecionar um atributo no banco de dados que tem um relacionamento 1:*, terá entradas duplicadas no dispositivo. Atributos com um relacionamento 1:1 (somente um atributo possível, como, por exemplo, Computer.System.Asset Tag), não mostrarão entradas duplicadas.

5. Para mudar a ordem das colunas, selecione um cabeçalho de coluna e clique em **Mover para cima** ou **Mover para baixo**.
6. Para remover uma coluna, selecione-a e clique em **Remover**.
7. Para alterar a posição apresentada para uma coluna, selecione a categoria, clique em **Editar**, faça suas alterações e pressione Enter . Não são suportados os seguintes caracteres estendidos: < , > , ' , " , !.
8. Clique em **OK** para salvar o conjunto de colunas.
9. Para usar a configuração de coluna personalizada ao ver uma lista de dispositivos, selecione a coluna e clique em **Definir como config de coluna atual**.

NOTA: Se estiver usando um banco de dados Oracle, selecione pelo menos um atributo definido nativamente pela análise de inventário (por exemplo, Computer.Display Name, Computer.Device Name, Computer.Device ID, Computer.Login Name, etc.).

Para editar um conjunto de colunas personalizadas

1. Na caixa de ferramentas do console Web, clique em **Administração > Preferências**.
2. Clique na guia **Colunas personalizadas**.
3. Selecione o conjunto de coluna personalizada e clique **Editar**.
4. Siga as instruções nos passos 4-8 acima para fazer mudanças.
5. Clique em **OK** para salvar suas mudanças.

Dicas de solução de problemas [console Web]

As seguintes dicas de resolução de problemas são para as questões que ocorrem com mais freqüência no Web Console.

Eu não sei a URL para o console Web.
Contacte a pessoa que instalou o servidor do núcleo, mais provavelmente o administrador de rede para o seu site. No entanto, normalmente o URL é http:// *core server machine nome* /remote.

Como estou conectado?
Observe a barra de título; o usuário que está logado é listada ao lado de **conectado como** .

A que máquina estou conectado?
Observe a barra de título; o nome do servidor do núcleo está listada ao lado de **Ligado a** .

Não estou a ver alguns dos links na barra.
Isso ocorre porque o administrador de rede é usando a administração baseada em papel ou função opção a nível de segurança que limita a realização de determinadas tarefas que você tem os direitos para fazer.

Tenho uma "permissão negada" erro quando eu tento acessar o console .
Para utilizar a segurança nível de funcionalidade no Windows 2000 e 2003, você deve desativar a autenticação anônima. Verifique as definições de autenticação do Web site e a .. \a LANDesk\ldsm pasta sob o site.

1. No servidor que é o host do Web console, clique em **Iniciar > Ferramentas administrativas > Gerenciador dos serviços de informações da Internet (IIS)**.
2. No menu de atalho do **Site da Web padrão** , clique em **Propriedades**.
3. Na guia **Segurança de diretório**, clique em **Editar** na caixa **Acesso anônimo e controle de autenticação.** Limpe a opção **Ativar acesso anônimo** e selecione **Autenticação integrada do Windows**.
4. Clique em **OK** para sair das caixas de diálogo.
5. Na sub-pasta **landesk\managementsuite** site padrão, clique em **Propriedades**. Repita os passo 3-4.

Obtenho uma sessão inválida ao abrir o console.
É possível que a sessão do navegador tenha expirado. Use o botão **Atualizar** do navegador para iniciar uma nova sessão.

Um erro de ASP.NET é exibido quando eu tento iniciar o Web console.
Se você ver uma mensagem de erro em ASP.NET quando tentar iniciar sessão na console Web, ASP e as permissões do diretório ASP não pode ser configurado corretamente. Redefina a configuração de ASP.NET executando o seguinte comando:

```
ASPNET_REGIIS.EXE -i
```

O número de itens por página é diferente do número que especifiquei.
Ao especificar quantos itens a exibir por página, essa definição é armazenada como cookies do navegador da Web e perde a validade quando a sessão terminar.

A sessão do console expira muito freqüentemente.
Você pode alterar o tempo de sessão padrão para as páginas console Web. O padrão do IIS é 20 minutos de inatividade antes de um login expirar. Para mudar o tempo limite da sessão IIS:

1. No servidor de web clique em **Iniciar > Ferramentas administrativas > Gerenciador dos Serviços de Informações da Internet (Gerenciador de IIS)**.
2. Expanda o **Site padrão**.
3. Clique com o botão direito do mouse na pasta **LDMS** e clique em **Propriedades**.
4. Na guia **Diretório virtual,** clique em **Configuração**.
5. Clique na guia **Opções de aplicativos** e, em seguida, altere o tempo limite da sessão para o valor desejado.

NOTA: Management Suite é um produto com base em sessão. Não desabilita o estado da sessão.

Não consigo ver a página do Controle remoto no web console.
Para visualizar a página do **Controle remoto**, você deve ativar os controlos ActiveX. Alguns navegadores têm os controles ActiveX desativados por padrão. Se a página do **Controle remoto** não carregar corretamente, ative os controles do ActiveX no seu navegador mudando as configurações de segurança.

Eu concluí o novo assistente do pacote de distribuição, mas o console não criou um pacote.
O console central utiliza as contas IUSR e IWAM no servidor de console. Essas contas são originalmente criadas com base no nome do computador. Se você mudar o nome do computador, é necessário seguir as etapas a seguir a fim de criar pacotes de software com êxito.

1. Se tiver instalado .Net Framework, desinstale-o.
2. Desinstale o IIS.
3. Reinstale o IIS.
4. Reinstale o .Net Framework se o tiver desinstalado.

Uma tarefa de distribuição de software agendada não foi executada.
Se você agendar um trabalho de distribuição de software e de ti não iniciar, verifique se o Intel® Local Scheduler serviço é executado no dispositivo.

Também, levar em consideração que a calendarização do trabalho baseia-se no tempo do servidor núcleo. Se a tarefa foi agendada em um console que reside em outra zona horária, a tarefa será iniciada com base na hora do servidor núcleo, que pode ser diferente da hora esperada.

Os gráficos do relatório não são exibidos corretamente.
A fim de visualizar os gráficos de pizza e barras interativos, exibidos em muitos relatórios, você precisa ter o Adobe Flash Player instalado. Verifique se o Flash está instalado e, em seguida, execute o relatório novamente.

Por que vejo duas instâncias do mesmo dispositivo no meu banco de dados?
Você excluiu um dispositivo a partir do banco de dados do núcleo e reinstalou usando UninstallWinClient.exe?

O UninstallWinClient.exe está no compartilhamento LDMain, que é a pasta principal do programa ManagementSuite. Apenas os administradores têm acesso a esse compartilhamento. Esse programa desinstala os agentes da LANDesk em todos os dispositivo onde é executado. Você pode mudá-lo para qualquer pasta que desejar ou adicioná-lo a um script de login. É um aplicativo Windows que é executado silenciosamente sem exibir nenhuma interface. Você pode ver duas instâncias do dispositivo no banco de dados que acabou de excluir. Uma dessa instâncias contém somente dados históricos,e a outra contém os dados de agora para o futuro.

Adicionei uma unidade S.M.A.R.T. em um dispositivo, mas não vejo a monitoração da unidade S.M.A.R.T. na lista de inventário para aquele dispositivo.
O monitoramento de hardware depende dos recursos do hardware instalado em um dispositivo, assim como da correta configuração do hardware. Se um disco rígido com capacidades de monitoração S.M.A.R.T. for instalado em um dispositivo mas a detecção S.M.A.R.T. não for habilitada nas configurações do BIOS do dispositivo, ou se o BIOS do dispositivo não suportar unidades S.M.A.R.T., os dados de monitoração não estarão disponíveis e não serão gerados alertas resultantes.

Nos scripts OSD DOS baseados em PXE, algumas partes após uma vírgula estão truncadas.
Em qualquer linha de um script, todos os personagens após a vírgula são truncados; por conseguinte, quaisquer comandos após a vírgula não são executados. Para evitar isto, use aspas em torno do comando completo, como este:

```
REMEXEC1=%QUOTE%echo "Oi,bom dia"%QUOTE%
```

Aspa simples não funcionará, pois são removidas na leitura do arquivo .INI.

Ao tentar instalar o Controle remoto do web console em uma sub-rede diferente, a tela do RC não pode ser instalada.
Se você se conectar com um console Web que está sendo hospedado por um núcleo em um domínio diferente, e clicar com o botão direito em um computador na lista **Meus dispositivos** e selecionar **Controle remoto**, você irá receber uma mensagem de erro dizendo que o visualizador de RC não foi adequadamente instalado.

Para resolver, o URL do CAB é obitido ao ler o marcador chamado "CabUrl" em web.config. O tag CabUrl deve incluir o nome de domínio totalmente qualificado do core ao invés de apenas o nome da máquina. Você precisa abrir o web.config e colocar o nome de domínio completamente qualificado no CabUrl.

Um dispositivo de disco USB não está listado na lista de inventário até um Análise de inventário tenha sido executado.
Quando um dispositivo de disco rígido está ligado por um cabo USB para um dispositivo gerenciado, não é imediatamente listada em discos rígidos no inventário do dispositivo. Ele é incluído sob as unidades lógicas após serem conectados ao dispositivo. Entretanto, ele não será mostrado em Disco rígidos até que seja feita uma análise de inventário no dispositivo.

Sobre os dispositivos gerenciados pelo Linux, um dispositivo de disco USB deve ser montado de forma a ser enumerados no inventário. Se ele for montado e não for feita uma análise de inventário, ele será mostrado sob os Unidade lógicas. Após a análise de inventário, eles serão incluídos também na lista de Discos rígidos. Quando o dispositivo é desconhecido ele deve ser desmontado do sistema. Em alguns sistemas Linux com kernel antigo, o dispositivo pode também ficar na lista de inventário mesmo após ter sido desconectado ou desmontado. Nesse caso o dispositivo gerenciado precisa ser reinicializado antes de ser removido da lista de inventário.

O mesmo endereço IP aparece duas vezes na lista Todos os dispositivos
Em dispositivos Linux em um segmento diferente do núcleo, você pode obter diversas entradas usando o mesmo endereço IP na lista Meus dispositivos. Para os nós no mesmo segmento de rede que o núcleo, a descoberta obtém o endereço MAC de um nó da Internet através do pacote ICMP. Para os nós que que não pertencem ao mesmo segmento de rede do núcleo, a descoberta obtém o endereço MAC de uma consulta NETBIOS. Como o Linux não responde a uma consulta NETBIOS, um endereço MAC não pode ser obtido de uma descoberta de análise de rede padrão para nós Linux em um segmento de rede diferente do núcleo. Quando um cliente é distribuído para um nó, o endereço MAC no arquivo de análise é usado para localizar o registro de inventário que será atualizado (após tentar usar o ID do dispositivo). Os registros que não possuem endereço MAC e ID de dispositivo não podem ser encontrados. Assim, um novo registro é criado. Você pode excluir a entrada duplicada na lista de dispositivos descobertos.

Exibição do console de Inventário e monitoração em tempo real [console Web].

Use o console de Inventário e monitoração em tempo real para visualizar as principais informações resumidas sobre um dispositivo, consulte as informações do sistema como a CPU ou ventilador, monitore o funcionamento e os limites dos componentes chace de um dispositivo, gerencie vulnerabilidades e acione, desligue ou reinicie o dispositivo.

O console do Inventário e monitoração em tempo real inclui as seguintes ferramentas:

- Informações do sistema
- Sessão remota
- Monitoração
- Conjuntos de regras
- Opções de ligar/desligar
- Configuração de hardware

NOTA: A fim de entender o console do Inventário e monitoração em tempo real de um dispositivo, você deve primeiro distribuir o agente de gerenciamento da LANDesk, com as seleções de componentes do Inventário e monitoração em tempo real, naquele dispositivo. O dispositivo também deve ser reinicializado após a instalação do agente para que o console de informações do servidor funcione corretamente. Essa

reinicialização é necessária quando você instalar o agente no servidor núcleo e nos dispositivos gerenciados.

Para ver o console de inventário em tempo real

1. No console do Management Suite, clique com o botão direito em um dispositivo gerenciado e selecione **Inventário e monitoramento em tempo real**.

   Você também pode clicar em **Ferramentas > Relatórios/monitorizamento > Dashboard de funcionamento** e clique duas vezes em um dispositivo na lista de dispositivos.

   O console abre em uma nova janela do navegador e mostra por padrão a página **Resumo do funcionamento**.

2. Clique nos botões de resumo do funcionamento para ver os detalhes sobre as informações de funcionamento do dispositivo.
3. Clique nos itens da caixa de ferramentas para utilizar as ferramentas disponíveis.

Informações do sistema

Informações do sistema contém dados do resumo sobre o funcionamento do dispositivo assim como informações sobre hardware e software, logs do sistema e outros dados como informações de recursos e da rede.

Resumo do funcionamento

A página **Resumo do funcionamento** fornece uma visão geral rápida do funcionamento do sistema para este dispositivo. Você pode ver rapidamente se os elementos de um determinado hardware estão funcionando corretamente e se há problemas potenciais que podem precisar de resolução.

Quando um dos elementos do funcionamento estiver em um estado de aviso ou crítico, o botão correspondente mostra um ícone amarelo (aviso) ou vermelho (crítico) indicando a existência de um problema. Clique no botão para ver a descrição do evento que causou o alerta de aviso ou crítico.

Resumo do sistema

Use a página **Resumo do sistema** para ver importantes informações sobre o dispositivo selecionado. As informações relacionadas na página podem incluir o seguinte, dependendo do tipo de hardware e software configurados no dispositivo.

- **Funcionamento:** O estado de funcionamento geral do dispositivo conforme definido pelas condições e parâmetros por você configurados.
- **Tipo:** O tipo do dispositivo, como, por exemplo, de impressão, de aplicativos ou de banco de dados.
- **Fabricante:** O fabricante do dispositivo.
- **Modelo:** O modelo do dispositivo.
- **Versão do BIOS:** A versão do BIOS do dispositivo.
- **Sistema operacional:** O sistema operacional do dispositivo.
- **Versão do SO:** O número da versão do sistema operacional.
- **CPU:** O fabricante, o modelo e a velocidade do processador do dispositivo.

- **tipo do IPMI, versão do IPMI:** O tipo e número da versão do IPMI que o dispositivo está usando.
- **Versão do BMC:** Para os dispositivos Intel AMT e vPro, este é o número da versão do controlador de gerenciamento da placa básica.
- **Versão do SDR:** A versão SDR (Sensor Data Record) no BMC do dispositivo.
- **Analisador de vulnerabilidades:** A versão do analisador de vulnerabilidade.
- **Controle remoto:** A versão do agente do controle remoto.
- **Distribuição de software:** A versão do agente da distribuição de software.
- **Analisador de inventário:** A versão do analisador de inventário.
- **Kernel:** O número da versão do kernel instalado para os dispositivos Linux.
- **Monitoração:** O número da versão do agente de monitoração do dispositivo.
- **Utilização da CPU:** Porcentagem em uso do processador.
- **Memória física usada:** A porcentagem do total de memória física utilizada no dispositivo.
- **Memória virtual usada:** A porcentagem do total de memória virtual utilizada no dispositivo.
- **Última inicialização*:** A data e o horário em que o dispositivo foi reinicializado pela última vez (de acordo com o fuso horário do banco de dados).
- **Unidade:** As unidades no dispositivo com o tamanho total da unidade e porcentagem de espaço utilizado.

Essas informações são obtidas no registro do Windows ou dos arquivos de configuração no Linux.

*Essa informação será exibida após o agente tiver sido instalado no dispositivo.

Hardware

Use a página **Hardware** para ver os detalhes sobre a configuração de hardware do dispositivo. Os itens na lista **Hardware** são agrupados nas seguintes categorias. Observe que nem todas as categorias são mostradas para todos os dispositivos. Por exemplo, se o dispositivo não tiver sensores de ventilador e temperatura, a categoria **Resfriamento** não é exibida nesta lista.

- **CPU:** processadores e cache
- **Armazenamento:** unidades lógicas, unidades físicas, mídias removíveis e adaptadores de armazenamento
- **Memória:** informações sobre o uso e módulos de memória
- **Chassis:** o chassi do servidor; mostra se a caixa está aberta ou fechada
- **Dispositivos de entrada:** teclado, mouse e outros dispositivos
- **Placa-mãe:** motherboard, slots de expansão e BIOS
- **Resfriamento:** sensores de ventilador e temperatura
- **FRUs:** Unidades de campo substituíveis (FRUs)
- **Alimentação:** Fontes de energia
- **Voltagem:** Voltagens
- **Sensores IPMI:** sensores discretos e numéricos
- **Dell DRAC:** dados do Dell DRAC. Clique nos botões para iniciar o Utilitário Dell DRAC e o administrador de servidor Dell DRAC.

Configuração dos limites de alerta para itens de hardware

Alguns itens na lista **Hardware** representam dados dos sensores no dispositivo, como os sensores de temperatura. Se um dispositivo gerenciado tiver componentes com sensores suportados, é possível mudar a leitura do sensor que disparou o alerta. Por exemplo, um sensor de temperatura de CPU pode ter leituras baixas e altas de temperatura que disparam os alertas de aviso e críticos. Os limites são normalmente baseados nas definições recomendadas do fabricante, mas você pode mudar as configurações altas e baixas usando a caixa de diálogo **Limites**.

1. Na caixa de ferramentas do Inventário e monitoração em tempo real, clique em **Informações do sistema.**
2. Expanda a pasta **Hardware** para encontrar o elemento de hardware que desejar (como **Resfriamento > Temperaturas**).
3. Na lista dos sensores, clique duas vezes no sensor ao qual desejar configurar limites.
4. Digite os valores nas caixas de texto de limites menores e/ou maiores ou arraste as barras para a esquerda ou para a direita para mudar os valores.
5. Clique em **Atualizar** para salvar suas mudanças.
6. Para voltar para os valores originais para os limites, clique em **Restaurar padrões**.

Logs

A página **Logs** mostra os logs dos sistemas locais, o SEL (System Events Log) para dispositivos IPMI e um log de alerta.

Os logs locais como os logs de **Aplicativo**, **Segurança** e **Sistema** têm um botão **Atualizar** para mostrar os dados mais atuais e um botão **Limpar** para remover todos os itens da lista.

Se o BIOS do dispositivo tem a capacidade de limpar o registro do **BIOS**, clique no botão **Limpar** para remover todas as entradas de registro. Esse botão não está disponível se o BIOS não suportar essa ação.

O log de **Alerta** mostra todos os alertas para o dispositivo. Você pode filtrar por nome, estado ou instância para reduzir o número de alertas na lista e pode habilitar o filtro de data para mostrar alertas de um intervalo específico de datas.

O log **Eventos de hardware** mostra dados em tempo real ou itens arquivados. Você pode excluir itens individuais, purgar todos os itens na lista ou atualizar a lista para mostrar a maioria dos itens de log recentes.

A página **Histórico de provisionamento** mostra o histórico de provisionamento do dispositivo, incluindo a data da ação de provisionamento, seu status e o modelo usado.

Software

A página **Software** mostra as informações de resumo sobre os processos, serviços e pacotes neste dispositivo, assim como uma lista de variáveis atuais de ambiente.

- **Processos:** mostra os processos que estão sendo executados; clique com o botão direito em um um processo e selecione **Eliminar processo** para encerrá-lo.
- **Serviços:** mostra os serviços disponíveis no dispositivo e seu status; clique com o botão direito em um serviço e selecione **Parar**, **Iniciar** ou **Reiniciar** para fazer as mudanças
- **Pacotes:** relaciona os pacotes instalados com números de versões e nome do fornecedor
- **Ambiente:** relaciona as variáveis de ambiente definidas no momento para o dispositivo

Outros

A página **Outro** mostra as informações sobre os recursos e um resumo do hardware e conexões da rede.

- **Informações de recursos:** Ver e editar as informações de gerenciamento de recurso. Clique em **Informações de contato** para inserir detalhes como nome e posição da pessoa que usa o dispositivo, além do local, departamento e o número de etiqueta de patrimônio do dispositivo. Clique em **Informações do sistema** para ver as informações do sistema como número de série, fabricante e tipo de gabinete
- **Informações da rede:** mostra uma lista do hardware de rede instalado, estatísticas da atividade na rede, um resumo de configuração (inclusive endereço IP, endereço padrão do gateway e informações sobre WINS, DHCP e DNS) e uma lista das conexões atuais da rede (unidades mapeadas)

Sessão remota

Use a **Sessão remota** para iniciar uma sessão de controle remoto com o dispositivo selecionado. Se o dispositivo for um servidor Windows, o controle remoto padrão é iniciado. Para servidores Linux, escolha entre sessões remotas SSH ou SFTP.

Na caixa de ferramenta do Inventário e monitoração em tempo real, clique em **Sessão remota** e em **Iniciar** para o a sessão de controle remoto.

Monitoração

Utilizar **Monitoramento** de exibição contadores de desempenho e definir limiares para componentes do dispositivo Os contadores de desempenho são usados com o alerta do **Monitor de desempenho** para monitorar eventos relacionados a desempenhos específicos em um dispositivo. Você deve distribuir um conjunto de regras de alertas para o dispositivo que inclua o alerta do Monitor de Desempenho para receber os alertas com base nos contadores de desempenho.

Para selecionar um contador de desempenho a monitorar

1. Em tempo real Inventário e monitoramento toolbox, clique em **Monitoramento**.
2. Clique na guia **Configurações do contador de desempenho**.
3. Na coluna **Objetos**, selecione o objeto que deseja monitorar.
4. Na coluna **Instâncias**, selecione a instância do objeto que deseja monitorar, se aplicável.
5. Na coluna **Contadores**, selecione o contador específico que deseja monitorar.
6. Especifique a freqüência de sondagem (polling) e o número de dias em que o histórico deverá ser mantido.
7. No campo **Alertar após o contador estar fora do intervalo**, especifique o número de vezes que o contador poderá ultrapassar o limite antes de ser gerado um alerta.
8. Especifique os limites superior e/ou inferior.
9. Clique em **Aplicar**.

Para ver um gráfico do desempenho de um contador monitorado

1. Clique na guia **Contadores de desempenho ativos**.
2. Na lista **Contadores**, selecione o contador do qual deseja ver um gráfico do desempenho.

3. Selecione **Visualizar dados em tempo real** para ver um gráfico do desempenho atual ou selecione **Visualizar dados do histórico** para ver um gráfico mostrando o desempenho durante o período que você especificou (usando a opção **Manter histórico** ao selecionar o contador).

No gráfico de desempenho, o eixo horizontal representa o tempo decorrido. O eixo vertical representa as unidades sendo medidas, como bytes por segundo (ao monitorar transferências de arquivos, por exemplo), Porcentagem (ao monitorar a porcentagem de CPU em uso) ou bytes disponíveis (ao monitorar o espaço em discos rígidos).

Conjuntos de regras

Use a ferramenta **Conjunto de regras** para ver uma lista dos conjuntos de regras de alerta atribuídos para o dispositivo selecionado e para ver os detalhes de cada alerta.

Para ver os conjuntos de regras de alerta

1. Na caixa de ferramentas do Inventário e monitoração em tempo real, clique em **Caixa de regras**.
2. Selecione um nome de conjunto de regras na lista suspensa para visualizar os detalhes dele.

As colunas de cada alerta são descritos abaixo.

- **Tipo de alerta:** uma descrição do evento de alerta monitorado.
- **Estado:** quando um evento de alerta atingiro status de severidade nesta coluna, um alerta será gerado. Cada evento pode ter vários status selecionados.
- **Ação:** A ação que ocorre quando o alerta é gerado, conforme definida na caixa de diálogo Conjunto de regras da ação.
- **Contribuição para o funcionamento:** se o evento de alerta atingir o estado especificado, o status de funcionamento do dispositivo muda na lista **Todos os dispositivos** ou no dashboard funcionamento.

Opções de ligar/desligar

Opções de ligar/desligar permitem desligar, reinicializar e, no caso de dispositivos IPMI e Intel vPro gerenciados, ligar dispositivos remotos. No caso de dispositivos que não sejam da IPMI, o dispositivo tem de ter o agente da LANDesk mobilizados para ela a fim de executar o reinicie e desligue as funções.

Com dispositivos IPMI e Intel vPro, você deve ter configurado as credenciais corretas para executar os recursos de ligar, desligar e reinicializar. Se IPMI ou dispositivos Intel vPro, o agente da LANDesk implantado, você pode executar o desligue e reinicie funções sem o IPMI ou Intel Vpro credenciais. Para configurar as credenciais BMC para dispositivos IPMI, use Configurar serviços.

Para utilizar as opções de ligar/desligar no dispositivo selecionado

1. Na caixa de ferramenta de Inventário e monitoração em tempo real, clique em **Opções de energia** .
2. Selecione **Reinicialização**, **Desligar** ou **Ligar** e clique em **Submeter**.

NOTA: Se tiver múltiplos servidores núcleo você pode usar opções de energia somente do servidor núcleo no qual conectou primeiro. Se você alternar para outro núcleo e tentar usar as opções de energia, o comando de alimentação não será bem sucedido.

Configuração de hardware

A ferramenta **Configuração de hardware** permite definir as opções para dispositivos com capacidade IPMI, Intel vPro e Dell DRAC. Essa ferramenta e quaisquer opções só são mostradas nos dispositivos com hardware correspondente (por exemplo, opções IPMI mostradas somente se o dispositivo for reconhecido como IPMI).

Usando o dashboard de funcionamento [console Web]

O dashboard (painel) de funcionamento é uma tela simples, de alto nível e organizada dos dispositivos. Ele representa cada dispositivo com um ícone que mostra o estado de funcionamento do mesmo. Os dispositivos que aparecem no dashboard funcionamento são baseados em escopos e funções. O dahsboard funcionamento é móvel e configurável. O painel de bordo de saúde apresenta a saúde geral de todos os dispositivos, o vista, listando o número de dispositivos por estado (número X de dispositivos em estado crítico, o número X de dispositivos em estado normal, e assim por diante). É possível ver um gráfico e uma lista de dispositivos, ou separar o gráfico e utilizá-lo sozinho na sua estação de trabalho ou monitor de grupo.

Quando você clica com o botão direito em um ícone do dispositivo, pode selecionar itens básicos de detecção e resolução de problemas, tais como: ping, route de rastreamento e controle remoto (se o dispositivo é gerenciado). Você também pode selecionar os detalhes da visão, o que abre o tempo real Inventário e monitoramento console.

- Para abrir o dashboard funcionamento
- Para exibir o console de Inventário e monitoração em tempo real.
- Para ver as propriedades do dispositivo
- Para executar tarefas básicas de solução de problemas
- Para classificar os dispositivos por nome ou estado de saúde
- Para ancorar o gráfico do dashboard funcionamento
- Para visualizar os dispositivos por categoria de status
- Para atualizar o dashboard funcionamento

Para abrir o dashboard funcionamento

1. No console do LANDesk Management, clique em **Ferramentas > Relatórios/Monitoração > Dashboard funcionamento**.

   O dashboard funcionamento abre-se em um navegador. Exibe os dispositivos listados em todo o **grupo de dispositivos**. Se os servidores estiverem relacionadas várias vezes e **Todos os dispositivos**, eles aparecerão da mesma forma no dashboard funcionamento.

2. Para evitar que dispositivos apareçam na lista várias vezes:
   - Configurar as opções de nome movimentação duplicada do dispositivo para configurar a LANDesk Software Serviços (em o LANDesk Management console, **> Serviços**)Configurar clique em .
   - Ao personalizar colunas na tela do dispositivo, evite escolher um atributo que resulte na exibição múltipla de um dispositivo na lista. Por exemplo, a seleção de aplicativos pode mostrar um dispositivo várias vezes, pois ele é incluído uma vez para cada aplicativo exclusivo de software instalado.

NOTA: Para os diálogos e o janelas para exibir corretamente, o servidor WebManagement Suite deve ser adicionado à lista de itens permitidos do bloqueador de pop-ups do navegador.

Para exibir o console de Inventário e monitoração em tempo real.

- No bordo de saúde, faça duplo-clique em um dispositivo.

O console do Inventário e monitoração em tempo real relaciona as informações básicas do inventário e do sistema, e tem uma opção de controle remoto e configurações de alerta de monitoramento e desempenho, além de opções de energia.

Para obter mais informações, consulte "Exibição do console de Inventário e monitoração em tempo real [console Web]." na página 902.

Para ver as propriedades do dispositivo

- No dashboard funcionamento, clique com o botão direito em um dispositivo e clique em **Propriedades**.

Ali são mostrados o nome do dispositivo, o endereço IP, a porcentagem de CPU e uso de memória e a quantidade de espaço restante no disco rígido. A tela **Propriedades** conecta ao dispositivo para coletar informações em tempo real de estatísticas importantes como espaço em armazenamento e memória usada.

Se o dispositivo estiver off-line (ou é incapaz de se comunicar na rede), a caixa de diálogo Propriedades relata um erro.

NOTA: Se o tempo real Inventário e monitoramento opção não é instalado com o agente da LANDesk em um dispositivo, a opção Propriedades não aparecem quando você clica com o botão direito do mouse no dispositivo.

Para executar tarefas básicas de solução de problemas

O dashboard funcionamento fornece funcionalidade básica de solução de problemas como, por exemplo, ping para o dispositivo, controle remoto (se o dispositivo for gerenciado) e o acesso ao console de informações do dispositivo.

1. Para controlar o dispositivo remotamente, clique com o botão direito no dispositivo e selecione **Controle remoto**.
2. Para fazer o ping de um dispositivo, clique com o botão direito do mouse no dispositivo e selecione **Executar ping no dispositivo)**.
3. Para enviar um comando de traçar rota ao dispositivo, clique com o botão direito no dispositivo e selecione **Tracert do dispositivo**.

Para classificar os dispositivos por nome ou estado de saúde

1. Na barra de ferramentas do painel de saúde, clique no **tipo de** lista pendente.
2. Selecione **Nome** ou **Funcionamento**.

Para ancorar o gráfico do dashboard funcionamento

1. Na barra de ferramentas do dashboard funcionamento, clique em **Docar gráfico**.

   Uma janela ancorável abre, que exibe o gráfico e as informações básicas do estado.

2. Para retornar o gráfico para a janela principal do dashboard funcionamento, clique no botão **Docar gráfico** novamente.

Para visualizar os dispositivos por categoria de status

1. Na barra de ferramentas do painel de saúde pública, clique na **lista pendente de ver**.
2. Selecione uma opção de estado de saúde (Normal, Aviso, crítica, ou todas).

NOTA: Você também pode clicar em um bar (ou seção de torta) no gráfico para exibir apenas os dispositivos correspondentes que status.

Para atualizar o dashboard funcionamento

Depois que você adicionar novos dispositivos para a **minha lista de dispositivos**, você deve manualmente atualizar a bordo da saúde para visualizar qualquer um destes novos dispositivos. Para fazer isso, clique no botão **Atualizar** na barra de ferramentas do dashboard funcionamento.

Essa ação adiciona e remove dispositivos da lista e atualiza o status de cada dispositivo. Não é preciso atualizar manualmente o dashboard funcionamento para ver o funcionamento do dispositivo atual. Quando o funcionamento de qualquer dispositivo monitorado muda, o dashboard funcionamento atualiza automaticamente seus ícones de dispositivo de forma a refletir o funcionamento atual do dispositivo.

Configuração das opções do dashboard funcionamento

Para configurar a forma como o painel de bordo de saúde exibe dados

1. Na barra de ferramentas do dashboard funcionamento, clique em **Opções**.
2. Digite um número (em segundos) na caixa **Atualizar a cada** para configurar a frequência com que o dashboard funcionamento checa as atualizações de status de funcionamento.
3. Selecione o tipo de gráfico que desejar na lista **Tipo de gráfico** (Barras 3D, Fatias 3D, Barras 2D, Fatias 2D).
4. Na lista **Visualizar**, selecione a categoria de status que desejar visualizar. Você pode abrir todos os dispositivos ou mostrá-los por tipo de status (Desconhecido, Aviso, Crítico, Crítico/Aviso).
5. Selecione a forma como os dispositivos devem ser ordenados (por Nome ou Funcionamento).
6. Selecione **Ícones grandes** para abrir o dashboard funcionamento com ícones grandes.
7. Selecione **Mostrar vista** para mostrar os dispositivos com as mesmas colunas do console principal. Os ícones grandes não aparecen nesta tela.
8. Clique em **OK**.

O status de funcionamento é atualizado de acordo com a frequência que você especificar neste diálogo. Se você quiser atualizar o status imediatamente, clique no botão **Atualizar** na barra de ferramentas.

Uso do controle remoto [console Web]

O controle remoto permite-lhe diagnosticar e solucionar problemas de dispositivos. Durante uma sessão remota, você pode fazer qualquer coisa no computador remoto que um usuário sentado no que poderia fazer, enquanto usando o layout do teclado de seu computador. Todas as suas ações ocorrem em tempo real naquele computador. O controle remoto permite:

- Resolver problemas de software e identificar os problemas de hardware rapidamente através da autorização de usuários para verificar e controlar remotamente um computador.
- Acessar arquivos remotos
- Transferir de arquivos nas duas direções
- Executar aplicativos remotos
- Reinicialização remota

Configure o acesso ao controle remoto a usuários com a ferramenta de Administração com base em funções. Se você possuir a segurança integrada ou baseada em certificados, o controle remoto direito poderá ser configurado para excluir os dias da semana e/ou as horas do dia. Se um usuário estiver controlando um computador remotamente e se uma restrição de horário tiver sido adicionada ao controle remoto corretamente, a sessão não funcionará após o fim do tempo da restrição.

Pré-requisitos para utilização do controle remoto

- Para usar o controle remoto do Console é necessário, primeiramente, instalar a tela do controle remoto. É necessário ter Privilégios administrativos no computador local para instalar a tela, que você deverá fazer download na primeira vez que acessar a página do controle remoto. Se necessário, é possível desinstalar a tela do controle remoto usando Adicionar/Remover programas no Painel de controle do Windows. Procure pelo **Console do controle remoto do**LANDeskManagement Suitena lista de programas.
- Para ser controlado remotamente, os dispositivos do Windows devem ter o agente de controle remoto instalado e carregado. Este agente é instalado por uma das seguintes ações:
    - Criar uma tarefa de configuração do agente no console e agendar o envio para o dispositivo
    - Mapear uma unidade entre o dispositivo e o servidor do núcleo e executar o agente apropriado configuração

  Este agente pode ser carregado como um serviço residente para fornecer acesso imediato ao computador, ou (se você tiver segurança baseada em certificado) pode ser instalado como um agente por demanda, que somente é carregado quando necessário.
- Além disso, você pode instalar o driver de espelhamento do controle remoto para melhorar o desempenho da detecção, captura e compactação nas mudanças do monitor se o CPU do dispositivo é mais lento (< 2,0 GHz) ou se a rede é rápida (> 100 MBbs) . Observe que o controle remoto não suporta gráficos DOS nem telas inteiras do DOS. A janela do prompt de comando pode não ser exibida inicialmente, ao usar o driver de espelhamento. Se isto ocorrer, minimize a janela e maximize-a.

Uso do controle remoto

Para controlar remotamente um dispositivo usando o console Web

1. Em qualquer lista **Meus dispositivos**, clique com o botão direito no ícone do dispositivo que você deseja conectar e selecione o **Controle remoto**.

   Você também pode selecionar o dispositivo e, no painel ação, clicar em **Propriedades> Controle remoto**.

   Esta ação abre o modo de exibição do Controle remoto da LANDesk. Outras opções remotas incluem controle remoto KVM para dispositivos Intel Vpro e 5 controle remoto baseado em navegador HTML.

2. Se você preferir usar um outro tipo de controle remoto, clique em **Acesso remoto > Controle remoto** na caixa de ferramentas do console Web. Selecione **Direct**, **KVM** ou **Baseado em navegador**, e especifique o nome do dispositivo ou do endereço IP do dispositivo que pretende controlar.

Você também pode controlar remotamente mais de um computador de cada vez. Após iniciar uma sessão, voltar para o console Web e selecionar outro computador.

Para obter informações sobre o controle remoto de dispositivos do Linux, veja "Acesso a dispositivos Linux remotos [console Web]" na página 917 .

Configuração da segurança de clientes Windows 2003 para o controle remoto

O serviço residente utiliza a segurança do Windows NT. Para funcionar em servidores Windows 2003, você deve configurar os clientes do servidor para que o modelo de segurança e compartilhamento do Windows 2003 para contas locais seja clássico (usuários locais autenticam-se como eles mesmos). Se isso não for feito, a autenticação padrão apenas como convidado não funcionará com a segurança do Windows NT do controle remoto.

Para configurar o modelo de segurança do Windows 2003 como clássico

1. No cliente Windows 2003, clique em **Iniciar > Painel de controle**.
2. No miniaplicativo **Ferramentas administrativas > Diretiva de segurança local**, clique em **Opções de segurança > Acesso à rede: Modelo de compartilhamento e segurança de contas locais**, e defina como **Clássico - usuários locais autenticam-se como eles mesmos**.

Controle remoto de dispositivos Windows [console Web]

Para iniciar o controle remoto

1. Em uma lista de dispositivos do console Web, selecione o dispositivo que quer controlar.
2. No painel de ações, clique na guia **Propriedades > Controle remoto**.

   Você também pode clicar com o botão direito do mouse no dispositivo e selecionar **Controle remoto**.

OLANDesk Controle remoto Visualizador abre.

Após controlar um dispositivo remoto, a tela desse dispositivo aparece na janela. Se o agente de controle remoto é carregado, o painel **Mensagens de conexão** no modo de exibição fornece informações de status.

Usando teclas de atalho no Controle remoto

Usar as teclas de atalho no visualizador do controle remoto

Para poder usar teclas de atalho, você precisa estar controlando um dispositivo remotamente.

1. Na janela do visualizador, digite a combinação de teclas do atalho correspondente a qualquer ação disponível.
2. Para acessar rapidamente as teclas de atalho, clique em **Enviar um botão especial de teclas da sequência na** barra de ferramentas e selecione um comando.

Para exibir os atalhos normalmente usados e alterar a sequência de teclas, clique na guia **Ferramentas > Opções > Configurações de teclas de atalho** na tela do controle remoto.

NOTA: Se as teclas de atalho não estiverem funcionando pode ser que o foco não esteja na janela do **Controle remoto**. Se a borda estiver azul/preta, o foco não estará na janela. Clique dentro da janela para mudar a cor da borda para amarelo/preto. As teclas de atalho estão agora habilitadas.

Enviar Ctrl+Alt+Delete para dispositivos Vista e Windows 7

A política de segurança local padrão do Windows Vista e Windows 7 não permitirá a sequência Ctrl+Alt+Delete vinda de uma tela de controle remoto. Para alterar isso, faça o seguinte.

Para permitir Ctrl+Alt+Delete em dispositivos Vista e Windows 7

1. Na caixa de pesquisa do menu **Iniciar** digite **gpedit.msc** e pressione **Enter**.
2. Navegue para **Diretiva do computador local > Modelos administrativos > Componentes do Windows > Opções de Logon do Windows > Sequência segura de software**.
3. Clique duas vezes em **Desabilitar ou habilitar Seqüência Segura de software**.
4. Clique em **Habilitar** e na lista **Opções** clique em **Serviços** ou **Serviços e aplicativos de fácil acesso**.
5. Clique em **OK**.

Navegar no monitor do dispositivo remoto

Por padrão, a Rolagem automática de tela está ativada. Rolagem automática quando é ativada e você está controlando remotamente um dispositivo, coloque o cursor ao longo da borda amarela/preta da janela do visualizador e desloque para cima, para baixo ou lado a lado. Quanto mais o cursor se aproximar da borda, mais rápida será a rolagem.

Você pode desativar Rolagem automática. Quando você faz isso, a borda amarela/preta é substituído por barras de deslocamento da janela se qualquer parte da tela do dispositivo remoto é obscurecida.

Para desativar a Rolagem automática no visualizador do controle remoto

1. Clique em **Ferramentas > Opções** e desmarque a caixa de seleção **Permitir Rolagem automática**.
2. Clique em **OK**.
3. Use as barras horizontais e verticais de navegação para mover o monitor do dispositivo remoto.

Desenho sobre a tela do dispositivo remoto

Você pode usar as ferramentas básicas de chamar a destacar uma área do monitor do dispositivo remoto. O usuário remoto vê o que lhe chamar, o que pode ser útil se você está mostrando algo para o usuário para ajudá-los a resolver um problema.

Para destacar parte da tela do monitor remoto com as ferramentas de desenho

1. No visualizador de controle remoto, clique no botão **Destacar uma área na tela remota**.
2. Use as opções na barra flutuante e desenhe no monitor remoto.

Utilizando uma sessão de bate-papo com o usuário remoto

Ao executar uma sessão de controle remoto, você pode abrir uma janela de bate-papo com o usuário remoto. Isto é útil quando você está ajudando alguém resolver um problema ou mostrando-lhes como para executar uma tarefa.

Para abrir uma janela de bate-papo com o usuário remoto

1. No visualizador de controle remoto, clique no botão **Iniciar/Para uma sessão** de bate-papo.
2. Digite um nome para a ação e clique em **Enviar**.
3. Para terminar a sessão de bate-papo, clique em **Parar** ou clique no botão na barra de ferramentas novamente.

A troca de mensagens é exibida na janela de bate-papo. Você pode salvar a sessão de bate-papo para referência futura.

Ver mensagens da conexão

O painel **Mensagens da conexão** na tela do visualizador exibe mensagens de status enviado para a barra de status (como agente pacote troca do controle remoto). As mensagens permanecem na lista, de forma que você pode:

- Visualizar o histórico da seção remota
- Diagnosticar problemas com a sessão
- Verificar se o agente de controle remoto está carregado
- Verificar o status do agente de controle remoto

Para ver as mensagens da conexão do console

- Se o **painel de mensagens da conexão** não for exibida, clique em **> Ligação Ver mensagens** .

Salvar mensagens da conexão

Na sessão de controle remoto você tem a opção de salvar as mensagens da conexão. Essas mensagens podem ser úteis como uma trilha de auditoria ou se você precisar solucionar quaisquer questões relacionadas com a sessão de controle remoto.

Para salvar mensagens da conexão

1. Na janela do visualizador, clique em **Arquivo > Salvar mensagens da conexão**.
2. Na caixa de diálogo **Salvar como**, digite um nome de arquivo e salve como arquivo de texto. Por padrão, as mensagens da conexão são salvas na pasta Meus documentos.

Se o agente do controle remoto estiver carregado, a janela **Mensagens de conexão** informará que o agente foi encontrado e qual protocolo está usando. Na lista de dispositivos do console Web, você também verá um ícone de lupa no dispositivo selecionado quando a sessão é criada.

Execução remota de programas

Na janela de exibição, você pode iniciar qualquer programa em um dispositivo remoto para diagnosticar problemas.

Para executar programas remotamente

1. Na caixa Executar da barra de ferramentas, insira o caminho para o programa que você quer executar. Se você precisa encontrar o programa, selecione **Procurar** na lista.
2. Para executar o programa no dispositivo remoto, clique no **controle remoto botão executar** da barra de ferramentas.

Transferência de arquivos para dispositivos remotos

Você pode usar a tela do controle remoto para transferir arquivos do seu computador para o dispositivo remoto. É como se tivesse mapeado uma unidade de um dispositivo remoto. No entanto, só é possível transferir arquivos para ou dos dispositivos tendo o agente de controle remoto instalado.

Este recurso funciona mesmo se não estiver utilizando o controle remoto no momento para controlar um dispositivo, desde que a conexão tenha sido criada. A **executar cada Explorador janela em uma** opção distinta do processo não funciona com a transferência do arquivo.

Para transferir arquivos para um dispositivo

1. Na barra de ferramentas do visualizador do controle remoto, clique em **Transferir arquivos para o computador remoto**.
2. Selecione um arquivo a ser transferido clicando no nome do arquivo. Clique o botão direito no arquivo e selecione **Copiar**, ou selecione para arrastar e soltar.
3. Role para baixo a árvore do Windows Explorer até chegar em **Controle remoto LANDesk**. Abaixo, clique no nome do dispositivo remoto que está controlando no momento.
4. No dispositivo remoto, abra uma pasta na qual o arquivo deve ser colado e clique com o botão direito do mouse e selecione **Colar**.

Da mesma forma, também é possível transferir arquivos de um dispositivo remoto para o seu dispositivo.

Desligamento e reinicialização de dispositivos remotos

Você pode desligar ou reinicializar remotamente os dispositivos. Ao fazer isso, aparece uma caixa de mensagens no dispositivo remoto, alertando-o de que o sistema será desligado em X segundos. Se alguém está nessa máquina, ele pode clicar em um **Desligar** ou no botão **Cancelar**.

Se nenhuma ação for tomada a reinicialização irá acontecer quando a contagem regressiva atingir 0.

Se alguns aplicativos estiverem abertos no dispositivo com dados que ainda não foram salvos, esses aplicativos provavelmente interromperão o desligamento quando solicitarem que o usuário os salve. Você pode ter que controlar remotamente o dispositivo e Salvar/Fechar aplicativos para que a reinicialização funcione.

Para reiniciar um dispositivo remoto

1. No visualizador do controle remoto, clique no botão **Reiniciar computador remoto** na barra de ferramentas.
2. Insira um período de tempo para exibir uma caixa de mensagem com o computador remoto (300 segundos no máximo).
3. Escreva uma mensagem para o usuário que irá aparecer na caixa de mensagem.
4. Para manter a ligação remota após a reinicialização, selecione o **Prosseguir sessão após** caixa de verificação de reboot.
5. Para manter as definições que introduziu como um padrão, selecione Salvar **estas configurações** caixa de verificação.

Configuração das opções de sessão

Existem várias definições que pode alterar para melhorar a sua utilização do visualizador remoto de controle, tais como alterar as opções de visualização, otimizando o desempenho de sua rede, e alterando os mapeamentos-chave para as teclas de atalho do computador remoto.

Para configurar as opções de sessões remotas

1. No visualizador do controle remoto, clique em **Ferramentas > Opções**.
2. Fazer alterações sobre as três páginas da caixa de diálogo, conforme abaixo descrito.
3. Ao terminar, clique em **OK**.

Guia Mudar configurações

- **Permitir rolagem automática:** Permite que a janela do controle remoto role conforme você move o cursor para perto da borda amarela/preta da janela. Quando esta opção estiver desmarcada, o dispositivo remoto janela tem barras horizontais e verticais de deslocamento se parte da janela é obscurecida.
- **Bloquear o teclado e o mouse remotos:** Bloqueia o teclado e o mouse do dispositivo remoto de modo que somente o usuário que estiver executando a janela do visualizador possa controlar o dispositivo remoto. Observe que as combinações de teclas especiais no Windows, como por exemplo "Ctrl+Alt+Delete" ou "Windows Key+L" não estão bloqueadas.
- **Sincronizar áreas de transferência**: Sincroniza as área de transferência do dispositivo local e remoto, para você possa colar informações entre os dois dispositivos.
- Ocultar a tela do computador remoto: Oculta a tela do dispositivo remoto de modo que somente o usuário que estiver executando o visualizador possa ver a tela da interface do usuário no dispositivo remoto.
- **Sempre peço para limpar tela do computador remoto:** Em vez de o automaticamente limpar a tela do dispositivo remoto, esta opção exibe uma caixa de mensagem para o usuário remoto para aceitar que a tela está apagada.
- **Bloquear o computador remoto quando a sessão terminar:** Bloqueia o dispositivo remoto quando a sessão termina, portanto, quem a esse dispositivo deve fornecer credenciais para usá-lo novamente.
- **Mapeamento automático de teclado:** Permite que o layout do teclado do console do vizualizador seja utilizado no dispositivo remoto.
- **Ativar compatibilidade com agentes antigos**: Se você deseja controlar um dispositivo remotamente com uma versão do agente da LANDesk mais antiga que a versão 8.5, marque esta caixa de verificação para ativar a ligação.
- **Uso de nomes alternativos:** Permite a utilização de nomes alternativos para a pessoa usando o visualizador de controle remoto, para que o login e computador nomes reais não aparecem no dispositivo remoto. Se tiver selecionado esta opção, digite os nomes alternativos nas caixas de texto abaixo.

Otimizar o desempenho para:

- **Otimizar o desempenho para**: Selecione Modem, Banda Larga, WIRELESS LAN, ou Personalizado, adequado para o seu ambiente de rede. (Estas opções estão também disponíveis na **otimização para** ferramentas de velocidade de ligação de desempenho botão.)
- **Usar driver de espelhamento no computador remoto:** Carrega o driver de espelhamento para melhoria do desempenho em máquinas mais lentas. Este driver pode reduzir o tempo necessário para

ver a área de trabalho da máquina alvo e aumentar a qualidade visual da imagem da área de trabalho em questão. Pode ser útil se o agente do controle remoto for obtido por download na Internet ou foi instalado em máquinas de usuários sem direitos de administrador.

- **Suprimir o papel de parede remoto:** Acelera a taxa de visualização por não exibir o padrão de fundo do dispositivo remoto. Alguns papeis de parede podem deixar a sessão de controle remoto lenta.
- **Reduzir a profundidade de cores:** Se você estiver conectando através de uma ligação lenta ou conexão dial-up networking, esta opção reduz a quantidade de informação transferida de cor. O mais perto que você mova o controle deslizante para redução completa, mais artefatos de cor (distorção) você pode ver.

Guia de configurações das teclas de atalho

Esta página da caixa de diálogo relacionada onze combinações de atalho usadas pela pessoa executando a sessão de controle remoto para enviar comandos para o computador remoto. Estas teclas de atalho são diferentes dos principais combinações padrão do Windows, pois entram as teclas padrão iria iniciar o comando no computador executando o visualizador do controle remoto, não o computador remoto.

Para alterar uma tecla de atalho, clique em na caixa e pressione a combinação de teclas que você deseja usar. A combinação de teclas (por exemplo, Ctrl+Shift+T) é inserido por você na caixa.

Acesso a dispositivos Linux remotos [console Web]

Para acessar um dispositivo Linux remotamente, pelo menos o agente padrão de gerenciamento deve ter sido implantado no dispositivo. Após selecionar um dispositivo Linux em qualquer lista de dispositivos da console Web, você tem uma escolha de **SSH e SFTP** para controle remoto.

NOTA: Se o dispositivo não teve nenhum agente implementado ainda e você selecionar um comando de **Controle remoto** do console Web, a tela de exibição do controle remoto do Windows é exibida porque o SO não é conhecido ainda. O espectador irá informar que não é possível ligar ao dispositivo.

Para acessar um dispositivo remoto Linux

1. Selecione o dispositivo na lista de dispositivos da console Web.
2. No painel da ação, clique na guia **Propriedades**.
3. Clique em **SSH** ou **SFTP.**

Se você selecionar acesso SSH, uma janela se abrirá com uma sessão SSH no dispositivo remoto. Forneça um nome de usuário e senha para acessar o dispositivo. Após ter autenticado, uma sessão de shell segura se abrirá no dispositivo remoto.

Se selecionar acesso SFTP, uma janela se abrirá com uma tela FTP segura do dispositivo remoto (baseada em uma conexão SSH). Forneça um nome de usuário e senha para acessar o dispositivo. Após ter autenticado, você pode usar a funcionalidade do FTP seguro para transferir arquivos entre seu computador e o dispositivo remoto.

Agendamento de tarefas [console Web]

A ferramenta **Tarefas agendadas** exibe as listas de tarefas de distribuição que você executou a partir do console de gerenciamento da LANDesk e do console Web. As tarefas podem incluir configuração do Agente, Patch Manager, distribuição de Software, aprovisionamento, Scripts e descoberta do dispositivo.

Na console Web, você pode programar os pacotes e scripts, tarefas do LaunchPad, diretivas e conjuntos de regras de alerta. As tarefas são apresentadas no painel de ação para cada recurso. Por exemplo, se você abrir a ferramenta **de distribuição**, você verá uma guia **Tarefas agendadas** no painel da ação que relaciona as tarefas de distribuição de pacotes. Tarefas para todas estas ferramentas também estão listados na ferramenta janela das tarefas agendadas.

NOTA: Enquanto você pode correr inventário, patch, e leituras de cumprimento da **minha** ferramenta de dispositivos, essas tarefas não são listados na ferramenta Tarefas agendadas. As mensagens de estado para estas leituras são exibidas no painel de ação apenas.

A ferramenta **Tarefas agendadas** é iniciada com a tarefa selecionada.

- **Minhas tarefas:** As tarefas que você agendou. Somente você e os usuários administrativos podem ver essas tarefas.
- **Tarefas públicas:** Tarefas que os usuários marcaram como públicas. Qualquer pessoa que editar ou agendar uma tarefa deste grupo, tornar-se-á o proprietária da tarefa. A tarefa permanece na pasta Tarefas públicas e também será visível no grupo Tarefas do usuário daquele usuário.
- **Todas as tarefas:** Suas tarefas e as tarefas marcadas como públicas.
- Todas as diretivas:
- **Tarefas do usuário** (Somente usuários administradores) Lista de todas as tarefas, ordenada por proprietário/criador (não incluindo tarefas públicos).

Quando você clica em **minhas tarefas**, **tarefas públicas** , ou **todas as tarefas** e a lista de tarefas mostra informações nestas colunas:

- **Tarefa:** Os nomes das tarefas.
- **Iniciar em:** Quando a tarefa está programada para execução. Clique sobre o nome da tarefa e clique em **Editar** para alterar o horário de início ou reprogramá-lo.
- **Status:** O estado geral de tarefas, que podem ser úteis, todas concluídas, nenhum preenchido, não programada, disponíveis para download, ou não.
- **Pacote de distribuição:** O nome do pacote que a tarefa distribui. Este campo só se aplica a pacotes de distribuição.
- **Método de entrega:** O método de entrega que a tarefa utiliza. Este campo só se aplica a pacotes de distribuição.
- **Proprietário:** O nome da pessoa que criou o pacote originalmente.
- **ID da tarefa**: Um número sequencial atribuído a tarefas no banco de dados.

Quando fizer duplo clique sobre uma tarefa agendada, o painel de ferramentas mostra esta informação de andamento:

- **Nome:** O nome do estado da tarefa.
- **Quantidade:** O número de dispositivos em cada estado da tarefa.
- **Percentagem:** A porcentagem de dispositivos em cada estado da tarefa.

Antes de poder agendar tarefas para um dispositivo, o agente padrão deverá estar instalado no dispositivo e o dispositivo deverá estar no banco de dados do inventário. Configurações de servidores são uma exceção. Eles podem visar um dispositivo que não tem o agente padrão de gerenciamento.

As tarefas podem ser remarcada, editado ou excluído, quer a partir da ferramenta Tarefas agendadas ou do painel de ação para a ferramenta específica. Para editar qualquer tarefa, selecione-a e clique no **botão Editar** na barra de ferramentas.

Criando grupos de tarefa personalizado

Você pode criar grupos personalizados para os tipos de tarefas **minhas tarefas** e **atribuições públicas** . Com grupos personalizados, você pode agrupar tarefas afins, tais como varredura de vulnerabilidades e executando um script

Para criar um grupo de tarefa personalizada

1. Na caixa de ferramentas do console Web, clique em **Distribuição > Tarefas agendadas**.
2. Selecione o grupo de tarefa para a qual pretende criar um grupo personalizado.
3. Clique no botão **Novo grupo** na barra de ferramentas.
4. Digite um nome para o grupo e clique em **OK**.
5. Para mover as tarefas ou outros grupos em grupo, selecione-os na lista e clique no botão Mover à barra de ferramentas. Selecione um grupo personalizado e clique em **OK.**

Transferência de tarefas

Use o botão **Mover** da barra de ferramentas para mover uma tarefa de um grupo-tarefa para outro, tornando assim a tarefa visível para os usuários que podem visualizar o grupo de tarefa que você está movendo a tarefa.

1. Na ferramenta **Tarefas agendadas** ou na guia de tarefas de uma ferramenta do console Web, selecione uma tarefa de um dos grupos (Minhas tarefas, Tarefas públicas, Todas as tarefas, Todas as diretivas ou Tarefas do usuário.
2. Clique no botão **Mover** na barra de ferramentas.
3. Selecione o grupo de tarefas para onde desejar transferir a tarefa, em seguida, clique em **OK**.

Ajuda do Agendador de Tarefas

As secções que se seguem descrevem as opções das caixas de diálogo relacionada à tarefa agendamento Web console.

- Página de Descrição Geral
- Página Scripts personalizados
- Página Dispositivos alvo
- Página Agendar tarefa
- Página do Pacote de distribuição
- Página Método de entrega
- Página Credenciais
- Página Informações da imagem
- Página de comandos adicionais
- Página do agente LANDesk
- Página Comandos de DOS

Sobre a página Descrição

- **Proprietário:** listas do atual proprietário da tarefa. Pode selecionar outro usuário como o proprietário, ou selecionar utilizador público ou públicos para salvar a tarefa do grupo público de tarefas.
- **Item selecionado:** exibe o nome do item a ser agendado. Clique em **Alterar** para abrir a página personalizada e selecione um item diferente.
- **Alvos selecionados:** exibe os dispositivos alvo da tarefa. Clique em **Alterar** para abrir a página de dispositivos alvo e alterar as metas.
- **A hora marcada:** será exibido quando a tarefa é agendada. Clique em **Alterar** para abrir a página da tarefa de programar e altere a hora.

Sobre a página Scripts personalizados

- **Script personalizado selecionado no momento:** Clique no script de rollup que deseja agendar.

Sobre a página Dispositivos alvo

Use esta página para adicionar os dispositivos alvo para a tarefa que você está configurando. Você pode ver os dispositivos alvo, consultas e grupos de dispositivos para a tarefa nesta guia.

Três listas suspensas incluir consultas, consultas LDAP, e os grupos que você criou noManagement Suite fim da rede.

- **Adição da lista alvo:** Adicionar os dispositivos que acrescentou à lista de alvo dos meus **dispositivos** . (Ver dispositivos alvos para obter instruções.)
- **Adição da lista LDAP:** Selecione um LDAP objeto que adicionou à lista de alvo a partir da árvore do **Gerenciador de Diretórios**.
- **Adicionar consulta:** Selecione a consulta na primeira lista e clique neste botão para adicionar os resultados da consulta à lista de alvo.
- **Adicionar consulta LDAP:** Marque uma consulta LDAP da segunda lista e clique neste botão para adicionar os resultados de uma consulta LDAP para a lista alvo.
- **Adicionar grupo:** Selecione um grupo na terceira lista e clique neste botão para adicionar o conteúdo do grupo à lista de alvo.
- **Ativar computadores:** Selecione esta caixa de verificação se quiser que a wake up dispositivos específicos (que são desligados ou em um sono ou estado de hibernação) quando a tarefa é iniciada.
- **Remover:** Selecione um item de destino e faça clique neste botão para remover esses dispositivos específicos.

NOTA: Na console Web, grupos de dispositivos não são orientados como grupos. Em vez disso, se selecionar um grupo e alvo, os dispositivos individuais no grupo são adicionados à lista alvo de dispositivos.

Sobre a página Agendar tarefa

- **Deixar sem agendar:** (padrão) Deixa a tarefa na lista Tarefas para agendamento futuro.
- **Iniciar agora:** Executa a tarefa assim que possível. Pode demorar até um minuto para a tarefa de iniciar, dependendo de outras configurações.
- **Iniciar na hora agendada**: Inicia a tarefa na hora em que você especificar. Especifique as seguintes opções:

- **Data**: O dia em que você deseja que a tarefa inicie.
- **Hora:** A hora em que você deseja que a tarefa inicie.
- **Repetir a cada:** Se você deseja que a tarefa de repetir, selecione o período (Hora, dia, semana ou mês). Se você escolher **mês** e a data não existe em todos os meses (por exemplo, 31) , a tarefa irá executar somente em meses que têm essa data.

- **Agendar estes dispositivos:** A primeira vez que uma tarefa é executada, deixe o padrão de **tudo** . Para execuções subseqüentes, escolha uma das seguintes opções.
  - **Dispositivos que não tiveram êxito:** Selecione esta opção somente se desejar que a tarefa seja executada em todos os dispositivos que não completaram a tarefa da primeira vez. Isto exclui os dispositivos com o status Bem-sucedido. A tarefa será executada em dispositivos em todos os outros estados, inclusive Aguardando ou Ativo. Considere o uso desta opção se precisar executar a tarefa no maior número possível de dispositivos que falharam, mas só é necessário que a tarefa seja completada com êxito uma vez em cada dispositivo.
  - **Aguardando ou atualmente trabalhando:** Selecione esta opção se desejar que a tarefa seja executada em dispositivos que estão aguardando para serem processados ou estão sendo processados no momento.
  - **Todos:** Selecione esta opção se desejar que a tarefa seja executada em todos os dispositivos, independentemente do estado do dispositivo. Considere o uso desta opção se você tiver uma tarefa, especialmente se for repetitiva, que precisa ser executada no maior número de dispositivos possível.
  - **Dispositivos que não tentaram executar a tarefa:** Selecione esta opção somente se desejar que a tarefa seja executada em dispositivos que não completaram a tarefa e nos quais não houve falha da tarefa. Isto exclui dispositivos que estavam com status Desligado, Ocupado, Com falha ou Cancelado. Considere o uso desta opção se houver um grande número de dispositivos alvo nos quais a tarefa falhou, e que não são importantes como alvos.

Sobre a página Pacote de distribuição

(Somente pacotes de distribuição) o pacote principal está selecionado por predefinição. Você pode alterar o pacote principal, selecionando-o e clicando no botão Remover. Você pode executar um outro pacote antes ou depois do pacote principal selecionando **Pacote preliminar** ou **Pacote final** e um pacote da lista.

- **Tipo:** O tipo de pacote para ser executado. Selecione um tipo da lista para visualizar os pacotes desse tipo disponíveis na caixa abaixo.
- **Pacote Preliminar:** Selecione esta opção para adicionar um outro pacote antes do pacote principal em uma distribuição multi-pacote. Selecione um tipo de pacote, encontre o pacote e clique em Configurar para adicioná-la à distribuição multi-pacote.
- **Pacote Principal:** O pacote primário a ser executado. Para alterar o pacote principal, selecione esta opção, selecionar um tipo de pacote, e encontrar o pacote. Clique em **Definir** para tornar o pacote principal.
- **Pacote Final:** Selecione esta opção para adicionar um outro pacote após o pacote principal em uma distribuição multi-pacote. Selecione um tipo de pacote, encontre o pacote e clique em Configurar para adicioná-la à distribuição multi-pacote.
- **Definir:** Clique neste botão para adicionar a opção de pacote selecionada à coluna Pedido.
- **Ordem:** A ordem em que os pacotes são executados. A ordem é Preliminar, Principal e Final.
- **Remover:** Remove o pacote selecionado do banco de dados.

Sobre a página Método de entrega

(Somente pacotes de distribuição)O método de distribuição define a forma como um pacote será enviado aos dispositivos.

- **Tipo:** Selecione o tipo de método de entrega (Compatível com a diretiva, Envio, Diretiva e Difusão seletiva) e selecione um método específico para esse grupo.
- **Método de entrega:** Selecione um método de entrega que você criou no Console de gerenciamento da LANDesk ou no console Web.

Sobre a página Credenciais

- **Nome de usuário:** identifica uma conta de usuário com as credenciais necessárias para o usuário iniciar a sessão no compartilhamento da rede.
- **Senha:** fornece a senha do usuário.
- **Domínio:** Fornece o domínio Ativar diretório ao usuário.

Sobre a página Informações da imagem

Use esta página para especificar o tipo de imagem que você deseja restaurar com este script, o local no qual a imagem será armazenada e o local no qual a ferramenta de criação de imagem está localizada:

- **Tipo de imagem:** Identifica o tipo de arquivo (formato do arquivo da imagem existente que você deseja distribuir com este script), selecionado na lista de ferramentas de criação de imagem.
- **Caminho UNC do arquivo de imagem a ser restaurado:** localiza o servidor e o compartilhamento nos quais o arquivo de imagem será armazenado, inclusive o nome do arquivo da imagem. A imagem deve ser armazenada em um compartilhamento acessível pelos dispositivos.
- **Caminho UNC da ferramenta de criação de imagem:** Localiza o servidor e o compartilhamento da ferramenta de criação de imagem (compatível com o tipo de imagem selecionado anteriormente), inclusive o nome do arquivo executável da ferramenta.

Sobre a página Comandos adicionais

- **Inserir os comandos a serem executados antes do cliente ser reinicializado e a imagem ser criada:** Insira comandos a serem executados antes do cliente ser reinicializado e a imagem ser criada.
- **Inserir parâmetros de linha de comando adicionais na ferramenta de criação de imagem:** Insira qualquer parâmetro adicional não especificado anteriormente.

Sobre a página do agente LANDesk

- **Caminho UNC:** O caminho para o pacote do agente.
- **Nome de usuário:** identifica uma conta de usuário com as credenciais necessárias para o usuário iniciar a sessão no compartilhamento da rede.
- **Senha:** fornece a senha do usuário.
- **Domínio:** Fornece o domínio Ativar diretório ao usuário.

Sobre a página Comandos de DOS

- **Comandos DOS:** Digite os comandos de DOS que desejar que sejam executados no dispositivo no momento da distribuição.
- **Abortar este trabalho se qualquer comando falhar:** Pára a tarefa se algum comando falhar e restaura o dispositivo ao estado anterior.

Exibição do log de alertas [console Web]

Use a página **Log de alertas** para ver os alertas enviados para o servidor núcleo. O log é ordenado pela hora (GMT) com o alerta mais recente na parte superior do log.

Para ver o log de alertas globais

1. Na caixa de ferramentas do console Web, clique em **Monitoramento > Log de alertas**.
2. Para ordenar as entradas por coluna, clique em um cabeçalho de coluna.
3. Para ver uma descrição mais detalhada do alerta, clique duas vezes na entrada, na coluna **Nome do alerta**.
4. Para listar as entradas de log por nomes de alertas, estado, instância, nome do dispositivo ou endereço IP, selecione os critérios na lista de **Filtro**. Por exemplo, selecione **Nome do alerta** e digite um nome completo (por exemplo, Desempenho) ou um nome parcial com o caractere curinga * (por exemplo, Remoto*) na campo filtro. Para fazer uma busca por data, selecione **Habilitar filtro de data** e insira uma data inicial e final. Ao adicionar critérios de filtro, clique no botão **Pesquisar**.
5. Para limpar o status de funcionamento de um alerta, selecione o alerta na coluna **Nome do alerta**, clique no botão **Reconhecimento** na barra de ferramentas e clique em **OK**.
6. Para excluir uma entrada de log, clique com o botão direito no alerta e clique em **Excluir entrada**.
7. Para eliminar todas as entradas no registro, clique com o botão direito na coluna **Nome de alerta** e selecione **Limpar log.**

NOTA: Se o nome do dispositivo não for mostrado como um nome de domínio totalmente qualificado, é porque este produto não conseguiu resolvê-lo para o dispositivo.

Clique aqui para ver as descrições das colunas de log de alertas.

- **Nome do alerta:** O nome associado ao alerta, conforme definido na página **Configurações de alerta**.
- **Hora:** A data e a hora em que o alerta foi gerado (GMT).
- **Estado:** O status de gravidade do alerta, que pode ser um dos seguintes:
  - **Desconhecido:** O status não pode ser determinado.
  - **Informativo:** Suporta mudanças de configuração ou eventos que os fabricantes incluem em seus sistemas.
  - **OK:** Indica que o status é um nível aceitável.
  - **Aviso:** Fornece algum tipo de advertência antecipada de um problema antes deste atingir um ponto crítico.
  - **Crítico:** Indica que o problema precisa de atenção imediata.
- **Instância:** Fornece mais informações detalhadas conforme a situação na qual o alerta foi gerado.
- **Nome do dispositivo:** O nome do dispositivo no qual o alerta foi gerado. Este deve ser um nome de domínio totalmente qualificado.
- **Endereço IP:** O endereço IP do dispositivo no qual o alerta foi gerado.

Uso de consultas [console Web]

Consultas são pesquisas personalizadas aos bancos de dados núcleo. As consultas ajudam a gerenciar a rede, permitindo que você pesquise e organize os dispositivos no banco de dados núcleo, com base em critérios específicos do sistema ou do usuário.

Por exemplo, você pode criar e executar uma consulta que capture somente dispositivos com uma velocidade do clock do processador menor do que 2 GHz ou com menos de 1.024 MB de RAM ou, então, uma unidade de disco rígido com menos de 80 GB. Crie uma ou mais instruções de consultas que representem essas condições e relacione as instruções umas às outras usando operadores lógicos padrão. Quando as consultas são executadas, é possível imprimir os resultados e acessar e gerenciar os dispositivos correspondentes.

EmManagement Suite você pode criar consultas do banco de dados para dispositivos em seu banco de dados do núcleo, e você pode criar consultas LDAP para dispositivos localizados em outros diretórios.

Na console Web, você pode criar consultas do banco de dados do núcleo utilizando a ferramenta **Consultas**. Você criar consultas LDAP com a ferramenta do gestor **de diretório**.

Visualizando as consultas disponíveis

A página de **Consultas personalizadas** exibe uma lista de consultas que você criou, na tela de rede da Management Suite ou no console Web.

Para visualizar as consultas disponíveis

1. Na caixa de ferramentas do console Web, clique em **Relatórios > Consultas**.
2. Expandir os grupos (as minhas consultas, consultas públicas, ou todas as consultas) para encontrar uma consulta.
3. Clique com o botão direito em uma consulta para editar, excluir ou executá-lo.

Executando consultas no console Web

Para executar uma consulta

1. Na caixa de ferramentas do console Web, clique em **Relatórios > Consultas**.
2. Expandir os grupos (as minhas consultas, consultas públicas, ou todas as consultas) para encontrar uma consulta.
3. Selecione uma consulta e clique no botão **Executar** na barra de ferramentas.

   Os resultados da pesquisa são exibidos no painel do aparelho.

4. Para imprimir os resultados das consultas, clique no botão **Imprimir tela** na barra de ferramentas. Os resultados da consulta completos são listadas em um formato de tabela. Utilize a função Imprimir do seu navegador para imprimir a lista.
5. Para guardar os resultados da pesquisa para um (valor separado por vírgula) arquivo CSV, clique no **botão Guardar como CSV** na barra de ferramentas e especificar um local para salvar o arquivo.
6. Para ver um resumo breve inventário de um dispositivo para os resultados da pesquisa, clique com o botão direito do mouse no dispositivo e clique em **computador da vista** .

NOTA: Se a consulta se estende de lista várias páginas, use as setas na parte superior direita da página para navegar entre as páginas. Digite o número de itens para mostrar por página e clique em **Definir**.

Criando consultas personalizadas [console Web]

As consultas personalizadas são úteis quando você deseja detalhes do inventário sobre o hardware e o software instalados nos dispositivos. Use uma consulta personalizada para criar uma lista de dispositivos com inventários semelhantes. Por exemplo, se quiser atualizar todos os dispositivo para um processador de pelo menos 2 GHz, você pode consultar todos os dispositivos no banco de dados com velocidades de processador menores do que 2 GHz. Consultas personalizadas também são utilizadas para definir grupos e escopos.

Você pode consultar qualquer dos itens do inventário (conhecidos como "atributos") que a varredura de inventário armazena no banco de dados.

Gerenciamento de consultas

Gerenciar consultas no painel ferramentas de **Consultas**. Utilize esta ferramenta para criar, editar ou excluir contatos:

- Para executar uma consulta existente, selecione-a e clique em **Executar**.
- Para criar uma nova consulta, clique em **Nova**. Depois que a consulta for criada e salva, seu nome aparecerá na lista dessa página.
- Para editar uma consulta na lista, clique duas vezes no nome da consulta. A página **Editar consulta** aparece com os parâmetros da consulta que você pode editar.
- Para editar a consulta mais recente, clique em **Editar a consulta atual**.
- Para excluir uma consulta, selecione-a e clique em **Excluir**.
- Para apagar os parâmetros da consulta da página **Editar consulta**, clique no botão **Limpar.** Caso a consulta já tenha sido salva, ela será limpa dessa página, mas permanecerá na lista **Consultas personalizadas**.

A criação de uma consulta é um processo de quatro etapas:

1. **Criar uma condição de pesquisa:** Especifica um conjunto de atributos de inventário que será a base de sua consulta.
2. **Selecionar os atributos a serem mostrados:** Refinar ou "filtrar" a consulta para que os resultados exibam os atributos mais útil para você, tais como endereços de IP ou nomes de dispositivo do computador.
3. **Classificar resultados por atributos:** Especifica como deseja ordenar os resultados da consulta. (Esta opção só se aplica se, na etapa 2, você escolheu para apresentar mais de um tipo de atributo nos resultados de consulta.)
4. **Executar a consulta:** Executa a consulta que você acabou de criar. Também é possível salvar a consulta para uso futuro ou eliminar todas as informações da consulta para começar novamente.

Passo 1: Criação de um critério de pesquisa [console Web]

Um critério de pesquisa é um conjunto de atributos de inventário e valores associados utilizado em uma consulta. Você pode usar um critério de pesquisa ou agrupar vários critérios para formar a base de uma consulta.

As etapas a seguir são executadas na página **Editar consulta**. Na tela **Personalizar consultas**, clique em **Nova**, ou selecione uma consulta existente e clique em **Editar**.

Para criar um critério de pesquisa:

1. Na caixa de ferramentas do console Web, clique em **Relatórios > Consultas**.
2. Na barra de ferramentas, clique em **Novo**, ou selecione uma consulta existente e clique em **Editar.**
3. No **Passo 1**, clique em **Editar**. Aparece uma janela mostrando uma lista que representa todos os dados de inventário armazenados no banco de dados no momento.
4. Percorra essa lista a fim de selecionar os atributos que constituirão seu critério de pesquisa. Por exemplo, para localizar todos os clientes que executam um determinado tipo de software, você deve selecionar Computer.Software.Package.Name.
5. Após selecionar os atributos, você vai ver uma série de campos no lado direito da janela. Nesses campos, selecione um operador e um valor para completar um critério de pesquisa. Por exemplo, para localizar todos os clientes o Internet Explorer 7.0 , selecione os atributos "Calculador.Software.pacote.Nome", o operador " = ", e o valor "Internet Explorer". Selecione o operador booleano E, em seguida, clique em **Adicionar** . Selecione os atributos "Computer.Software.Package.Version", o usuário "LIKE", e o valor "8" e clique em **Adicionar**.
6. Você pode continuar a refinar a consulta criando outro critério de pesquisa e, em seguida, adicionando-o ao primeiro critério com um operador booleano (AND ou OR). Você também pode usar os botões para adicionar, excluir, substituir, agrupar ou desagrupar os critérios criados.
7. Ao concluir, clique em **OK**.

NOTA: Para executar e armazenar uma consulta sobre o status de funcionamento de servidores (Computer.Health.State), é preciso estar alerta para o fato de que o estado no banco de dados é representado por um número. Use a tabela abaixo para criar condições de busca. Por exemplo, para criar uma condição de busca para computadores com estado de funcionamento "Desconhecido", use o operador "NOT EXIST".

Condição de funcionamento	Operador
Desconhecido	NOT EXIST
Normal	2
Aviso	3
Crítico	4

Etapa 2: Seleção dos atributos a serem exibidos [console Web]

Para a Etapa 2, selecione os atributos que serão úteis para identificar os computadores incluídos nos resultados da consulta. Por exemplo, se quiser resultados que o ajudem a localizar fisicamente cada computador correspondente ao critério de pesquisa definido na Etapa 1, especifique atributos como, o nome de exibição de cada computador (Computer.DisplayName) ou endereço IP (Computer.Network.TCPIP.Address).

Para selecionar os atributos a serem mostrados:

1. Na página **Editar consulta**, no **Passo 2,** clique em **Editar.** Aparece uma janela mostrando uma lista que representa todos os dados de inventário armazenados no banco de dados no momento.
2. Percorra essa lista a fim de selecionar um atributo a ser mostrado na lista de resultados da consulta. Lembre-se de selecionar atributos que ajudarão a identificar os clientes retornados na consulta.

NOTA: Se estiver usando um banco de dados Oracle, selecione pelo menos um atributo definido nativamente pela análise de inventário (por exemplo, Computer.Display Name, Computer.Device Name, Computer.Device ID, Computer.Login Name, etc.).

3. Depois que você tenha selecionado um atributo, clique em **Adicionar** para movê-la para a caixa na metade inferior da janela.
4. Se pretender enumerar a sua consulta lista de resultados, selecione **Incluir uma contagem** .
5. Repita o processo para adicionar atributos mais. Utilize os botões de seta para baixo para adicionar ou remover atributos e, em seguida, clique em Mover **para cima ou Mover para baixo para** alterar a ordem dos atributos.
6. Para permitir que os resultados da consulta sejam direcionáveis para qualquer ação que você especificar, selecione **Transforme os resultados em alvos**.
7. Ao concluir, clique em **OK**.

Você também pode editar os cabeçalhos de coluna na sua consulta lista de resultados.

Para alterar cabeçalhos de coluna

1. No **Passo 2**, clique em **Editar**.
2. Na caixa inferior, clique num cabeçalho de coluna e clique em **Editar**. Edite o cabeçalho e pressione **Enter**. Repita o procedimento, se necessário.
3. Clique em **OK**.

Neste ponto, você pode querer salvar a consulta. O próximo procedimento de criação de uma consulta é opcional e se aplica apenas aos resultados da consulta que contêm duas ou mais colunas. Para salvar a consulta, clique no botão **Salvar** na barra de ferramentas. Digite um nome para o **Salvar consulta** caixa de diálogo, selecionar um grupo e, em seguida, clique em **Salvar**.

Passo 3: Classificação de resultados por atributo [console Web]

Este passo só é necessário se você definir mais do que um atributo e cabeçalho de coluna no Passo 2 e agora pretende ordenar os resultados por ordem alfabética ou numérica dentro de uma dessas colunas.

Por exemplo, se você especificou dois atributos diferentes para exibir os resultados de consulta (o endereço IP e o tipo de processador), você poderia classificar em ordem alfabética por tipo de processador, os resultados.

Caso você pule essa etapa, a consulta será ordenada automaticamente pelo primeiro atributo selecionado na Etapa 2.

Para ordenar os resultados por atributo

1. Na página **Editar consulta**, no **Passo 3,** clique em **Editar.** Aparecerá uma janela mostrando os atributos que você selecionou no **Passo** 2.
2. Selecione o atributo pelo qual deseja classificar e clique em **>>** para mudá-lo para a caixa **Atributos selecionados** vazia.
3. Clique em **OK**.

Etapa 4: Executando a consulta [console Web]

Após criar sua consulta, você pode executá-lo, guardá-lo, ou claro, para começar.

Para salvar a consulta para utilização futura

1. No **Editar consulta** página, clique no **botão da barra de salvar**. A consulta aparece agora na lista da página **Consultas personalizadas**.
2. Se a sua consulta é uma versão modificada de um outro, clique no botão **Guardar como** da barra de ferramentas para dar-lhe um novo nome.

Por padrão, as consultas salvas só podem ser visualizadas pela pessoa que as salvou. Se você selecionar **Consulta pública** antes de salvar, a consulta salva será visível para todos os usuários. Somente administradores com o direito Gerenciamento de consultas públicas pode tornar pública uma consulta.

Para imprimir os resultados de uma consulta

- Clique no botão da barra de ferramentas **Nova**.

NOTA: Relatórios de consultas são executados na ordem indicada. Se nenhum agrupamento for feito, o relatorio são executados de baixo para cima. Agrupe itens de consultas relacionadas para que elas sejam avaliadas como um grupo. Caso contrário, os resultados de sua consulta podem ser diferentes do esperado.

Visualizar resultados da consulta [console Web]

Os resultados correspondem aos critérios de pesquisa que foram especificados no processo de criação da consulta. Se os resultados não forem os esperados, retorne à página **Editar consulta** e refine as informações.

Para visualizar a informação do inventário sobre um dispositivo nos resultados de consulta

- Clique com o botão direito no dispositivo e selecione **Exibir computador**.

Para imprimir os resultados de uma consulta

1. Clique no botão **Imprimir tela** na barra de ferramentas. Os resultados da consulta completos são listadas em um formato de tabela.
2. Utilize a função Imprimir do seu navegador para imprimir a lista.

Salvar um relatório como um arquivo CSV

1. Clique no **botão Guardar como barra de CSV**.
2. Especifique onde deseja salvar o arquivo.

Exportar resultados da consulta para um arquivo CSV [console Web]

Para visualizar os resultados da pesquisa em uma planilha ou em outro aplicativo, exporte os dados como um arquivo CSV (valor separado por vírgula).

Salvar um relatório como um arquivo CSV

1. Na página de resultados da consulta, clique no **botão Guardar como** ferramentas de CSV.
2. Especifique onde deseja salvar o arquivo.

Exportação e importação de consultas [console Web]

Você pode exportar e importar quaisquer consultas que criar. Todas as consultas são exportadas como arquivos XML.

Os recursos exportar e importar são úteis em duas situações:

- Se for necessário reinstalar seu banco de dados, use os recursos exportar/importar para salvar as consultas existentes a fim de serem usadas em um novo banco de dados.

  Por exemplo, você pode exportar as consultas e movê-los para um diretório afectada por uma reinstalação de dados. Após reinstalar o banco de dados, é possível mover as consultas novamente para o diretório de consultas no seu servidor web e importá-las para seu novo banco de dados.

- Os recursos exportar/importar podem ser usados para copiar consultas para outros bancos de dados.

  Por exemplo, você pode exportar uma consulta para um consulta diretório no seu servidor Web, e depois enviá-lo para outro administrador da LANDesk. Essa pessoa poderia colocar as consultas no diretório de consultas em um outro servidor da Web e importá-los para um banco de dados diferente.

Para exportar uma consulta

Conclua essas etapas ainda conectado a um banco de dados que tenha uma consulta que você quer exportar.

1. Na caixa de ferramentas do console Web, clique em **Relatórios > Consultas**.
2. Na página **Consultas personalizadas**, clique no nome da consulta a ser exportada. Clique no botão **Editar** na barra de ferramentas.
3. No **Editar consulta** página, clique na **barra de ferramentas do botão Exportar**. A página **Consultas exportadas** é exibida.
4. Para visualizar o documento XML para a consulta, clique no link do documento XML.
5. Para salvar o documento XML, clique com o botão direito do mouse no link e selecione **Salvar alvo como**. Especifique um local para salvar o arquivo.

Para importar uma consulta

Execute estas etapas ainda conectado a um banco de dados para o qual deseja importar uma consulta.

Para importar uma consulta em um banco de dados, a consulta deve ser nas consultas diretório reconhecido pelo servidor Web. Por padrão este diretório é c:\inetpub\wwwroot\LANDesk\LDMS\queries.

1. Na caixa de ferramentas do console Web, clique em **Relatórios > Consultas**.
2. Na página **Consultas personalizadas**, clique em **Novo** da barra de ferramentas.

3. Na página **Editar consulta**, clique no botão **Importar** da barra de ferramentas.
4. Selecione a consulta a ser importada. Se você quiser verificar os parâmetros da consulta antes de importar, faça clique no botão Ver da barra de ferramentas.
5. Clique em **Importar** para importar a consulta. Se pretender importar todos os contatos na lista, clique em **Importar tudo** .

Criando consultas LDAP usando o gerenciador de diretórios [console Web]

Além da capacidade de consultar o banco de dados do núcleo com consultas de banco de dados, você também pode usar a ferramenta **Gerenciador de diretórios** para localizar, acessar e apontar para dispositivos em outros diretórios via LDAP (Lightweight Directory Access Protocol).

Você pode consultar dispositivos com base em atributos específicos, como tipo de processador ou SO. Também é possível executar uma consulta com base em atributos específicos do usuário, como ID ou departamento do funcionário.

Adicionando um diretório LDAP

Para gerenciar um diretório LDAP, você precisa adicioná-lo à lista de gestor do Diretório. Para o fazer, precisa de saber a localização do diretório sobre a rede e um conjunto de credenciais para acessar o diretório.

Para adicionar um diretório LDAP para gestor de lista telefónica

1. Na caixa de ferramentas do console Web, clique em **Distribuição > Gerenciador de diretórios**.
2. Clique no botão **Novo diretório** na barra de ferramentas.
3. Digite o URL para acessar o diretório. Você não precisa digitar o " : //inicial LDAP " na URL.
4. Digite um nome de usuário e uma senha válidos para acessar o diretório.
5. Clique em **OK**.

O diretório está listado com um ícone de árvore no painel de ferramentas do gestor de lista telefónica. Você também pode selecionar o diretório e clique no botão Editar na barra de ferramentas para exibir suas propriedades.

Exibindo diretórios LDAP

Quando você tiver completado, pelo menos, um diretório, você pode ver os itens no diretório na vista de árvore do gestor do Diretório, que exibe todos os diretórios e usuários cadastrados.

Existem duas guias no painel de ações, **Lista de LDAP alvo**e **Consultas LDAP**. Clique sobre eles para visualizar objetos LDAP que foram orientadas e consultas LDAP que você definiu.

Apontando para objetos LDAP

Você pode selecionar objetos na árvore de gerenciador de listas e meta-los. Os dispositivos contidos em tais objetos de LDAP podem ser selecionados como alvos de uma ação, como a distribuição de software ou análises de patch e conformidade.

Para apontar para objetos LDAP

1. Na caixa de ferramentas do console Web, clique em **Distribuição > Gerenciador de diretórios**.
2. Navegue pela árvore do **Gerenciador de diretórios** e selecione um objeto no diretório LDAP.

3. Selecione um ou mais itens da **recursos da lista do diretório** e clique no botão **de metas do LDAP** na barra de ferramentas.
4. Tem certeza de que deseja aplicar aos dispositivos alvo Os itens que você visados são exibidas na **opção da lista de alvo para** a ferramenta.

Criando uma consulta ao diretório LDAP

Você pode criar uma consulta que retorna resultados para um objeto do Active directory, como uma organização de raiz (ó), domínio componente (dc), ou unidade organizacional (uo).

Para criar uma consulta de LDAP:

1. Na caixa de ferramentas do console Web, clique em **Distribuição > Gerenciador de diretórios**.
2. Navegue pela árvore do **Gerenciador de diretórios** e selecione um objeto no diretório LDAP. A consulta que você está criando retornará resultados a partir desse ponto da árvore para baixo.
3. Clique no botão **Nova consulta LDAP** da barra de ferramentas.
4. Digite um nome descritivo para a consulta.
5. Selecione um atributo de LDAP que será um critério para a consulta.
6. Clique um operador de comparação para a consulta (=, <=, > =) e um valor para o atributo. Se você selecionar **contém** ou **existe,** nenhum valor é necessário.
7. Se a consulta for complexa, selecionar **E** ou **OU** para unir os resultados.
8. Clique em **Inserir** para adicionar o relatório.
9. Criar resultados adicionais repetindo as etapas 5-8 .
10. Para negar um relatório, selecione-o, depois clique em **NÃO**. Para excluir um relatório, selecione-o e clique em **Excluir**.
11. Quando a consulta estiver concluída, clique em Testar para verificar se os resultados da consulta de retorno.
12. Se você deseja editar a consulta e utilização freeform sintaxe do LDAP, clique em Avançadas. A consulta é aberta em uma janela de edição que lhe permite usar quaisquer opções sintaxe.
13. Ao concluir, clique em **Salvar**. A consulta salva será exibida na guia **Consultas LDAP**, no painel de ações do Gerenciador de diretórios.

Sobre a caixa de diálogo Consulta LDAP avançada

Na caixa de diálogo Consulta LDAP básica, clique em **Avançada** para abrir a caixa de diálogo Consulta LDAP avançada. A caixa de diálogo Consulta LDAP avançada é exibida quando você opta por editar uma consulta que já tenha sido criada.

- **Nome:** O nome da consulta LDAP. Editar o nome para criar uma cópia de uma consulta existente.
- **Raiz da consulta LDAP:** Exibe o objeto raiz no diretório para esta consulta. A consulta que você está criando retornará resultados a partir desse ponto da árvore para baixo.
- **Consulta LDAP:** Criar uma consulta LDAP de forma definidor.
- **Teste:** Clique para executar um teste da consulta que você criou.

Mais sobre o LDAP (Lightweight Directory Access Protocol - Protocolo de acesso a diretório leve)

LDAP é um protocolo de padrão da indústria para acessar e visualizar informações sobre usuários e dispositivos. O LDAP permite que você organize e armazene essas informações em um diretório. Um diretório LDAP é dinâmico, pois pode ser atualizado conforme a necessidade e é distribuído, protegendo-o de um único ponto de falha.

Os exemplos a seguir mostram consultas LDAP que podem ser usadas para pesquisar o diretório:

- Obter todas as entradas: (objectClass=*)
- Obter entradas contendo 'bob' em qualquer lugar do nome comum: (cn=*bob*)
- Obter entradas com um nome comum maior ou igual a 'bob': (cn>='bob')
- Obter todos os usuários com um atributo de e-mail: (&(objectClass=user (email=*)
- Obter todas as entradas de usuários com um atributo de e-mail e um sobrenome igual a 'smith': (& (sn=smith (objectClass=user (email=*)
- Obter todas as entradas com um nome comum que comece com 'andy', 'steve' ou 'margaret': (& (objectClass=User (| (cn=andy* (cn=steve* (cn=margaret*)
- Obter todas as entradas sem um atributo de e-mail: (!(email=*)

A definição formal do filtro de pesquisa é a seguinte (em RFC 1960):

- <filter> ::= '(' <filtercomp> ')'
- <filtercomp> ::= <and> | <or> | <not> | <item>
- <and> ::= '&' <filterlist>
- <or> ::= '|' <filterlist>
- <not> ::= '!' <filter>
- <filterlist> ::= <filter> | <filter> <filterlist>
- <item> ::= <simple> | <present> | <substring>
- <simple> ::= <attr> <filtertype> <value>
- <filtertype> ::= <equal> | <approx> | <ge> | <le>
- <equal> ::= '='
- <approx> ::= '~='
- <ge> ::= '>='
- <le> ::= '<='
- <present> ::= <attr> '=*'
- <substring> ::= <attr> '=' <initial> <any> <final>
- <initial> ::= NULL | <value>
- <any> ::= '*' <starval>
- <starval> ::= NULL | <value> '*' <starval>
- <final> ::= NULL | <value>

O símbolo <attr> é uma seqüência de caracteres que representa um Tipo de atributo. O símbolo <value> é uma seqüência de caracteres que representa um Valor de atributo cujo formato é definido pelo serviço de diretório subjacente.

Se o <value> precisar conter um dos caracteres * ou (or), use uma barra invertida (\) antes do caractere.

Gerenciamento de inventário [console Web]

Você pode usar inventário digitalização para visualizar hardware e software dados para dispositivos gerenciados. Os dados do inventário são armazenados no banco de dados núcleo. Isso inclui hardware, o driver do dispositivo, software, memória e meio ambiente informações. Use o inventário para ajudar a gerenciar e configurar dispositivos e a identificar problemas no sistema rapidamente.

Você pode ver, imprimir e exportar os dados de inventário. Também é possível usá-lo para definir consultas, agrupar dispositivos e gerar relatórios especializados.

Visão geral da análise de inventário

Ao configurar um dispositivo com um agente de gerenciamento da LANDesk, o analisador de inventário é um dos componentes do agente instalados no dispositivo. Quando você cria uma configuração do agente, pode-se especificar quando o scanner de inventário é executado no dispositivo.

A análise de inventário é automaticamente executada quando o dispositivo é inicialmente configurado. O executável do scanner é denominado.exe ldiscn32 para dispositivos Windows e ldiscn para dispositivos do Linux. A análise de inventário coleta os dados de hardware e software e os insere no banco de dados núcleo. Depois disso, a verificação de hardware funciona no intervalo especificado (por padrão, é executado uma vez por dia).

Para definir as configurações de análises de software

1. No servidor núcleo, clique em **Iniciar > Todos os programas > LANDesk > Configurar serviços da LANDesk**.
2. Clique na guia **Inventário**.
3. Para alterar a frequência de leituras de software, clique em **Software** .
4. Faça quaisquer outras mudanças que você gostaria (clique em Ajuda para obter descrições das opções).
5. Ao concluir, clique em **OK**.

Após a análise inicial, a análise de inventário pode ser executada do console como uma tarefa agendada. O agente padrão de gerenciamento deve estar em execução nos dispositivos remotos para agendar uma análise de inventário.

NOTA: Um dispositivo adicionado ao banco de dados núcleo, usando a ferramenta Descoberta de descoberta de dispositivos não gerenciados ainda não analisou seus dados de inventário no banco de dados núcleo. É preciso executar uma varredura de inventário em cada dispositivo para que todos os dados de inventário sejam exibidos para esse dispositivo.

Você pode ver os dados de inventário e usá-los para:

- Personalizar as colunas da lista **Todos os dispositivos** para exibir os atributos de inventário específicos
- Consultar o banco de dados núcleo quanto a dispositivos com atributos de inventário específicos
- Agrupar dispositivos para designar tarefas de gerenciamento, como distribuição de software
- Gerar relatórios especializados com base nos atributos de inventário
- Manter o controle das mudanças de hardware e software nos dispositivos e gerar alertas ou entradas no arquivo de log quando essas mudanças ocorrerem.

Análise delta

Depois que a análise completa inicial é executada em um dispositivo Windows, uma execução subseqüente da análise de inventário captura apenas as modificações delta e as envia ao banco de dados núcleo. Use a opção do analisador /RSS para coletar informações de software no registro do Windows. (Esta opção não se aplica aos dispositivos Linux.)

Como forçar uma análise completa

Se quiser forçar uma análise completa dos dados de hardware e software do dispositivo Windows, você pode apagar o arquivo delta de análise atual e mudar um parâmetro em Configurar serviços de software LANDesk. (Esta opção não se aplica aos dispositivos Linux.)

1. Exclua o arquivo **invdelta.dat** do dispositivo. Há uma cópia da última análise de inventário armazenada localmente como arquivo oculto denominado invdelta.dat A variável de ambiente LDMS_LOCAL_DIR define o local desse arquivo. Como padrão o local é C:\Arquivos de programa\LANDesk\LDClient\Data.
2. Adicione a opção **/sync** à linha de comandos do utilitário de análise de inventário. Para editar a linha de comandos, clique em **Iniciar > Todos os programas > LANDesk Management**, clique com o botão direito no ícone de atalho **Análise de inventário**, selecione **Propriedades > Atalho** e, em seguida, edite o caminho **Alvo**.
3. No servidor núcleo, clique em **Iniciar > Todos os programas > LANDesk > Configurar serviços LANDesk**
4. Clique na guia **Inventário** e clique em **Configurações avançadas**.
5. Clique no parâmetro **Do Delta** (Executar Delta). Digite **0** na caixa **Valor**.
6. Clique em **OK** duas vezes e clique em **Sim** ao ser avisado para reiniciar o serviço.

Compactação da análise

As análises de inventário executadas pela análise de inventário do Windows (ldiscn32.exe) são compactadas por padrão. A análise compacta as análises completas e delta com uma taxa de compactação de aproximadamente 8:1. Em primeiro lugar, as análises são compiladas totalmente na memória, em seguida, são compactadas e enviadas ao servidor núcleo usando um tamanho de pacote maior. A compactação da análise requer menos pacotes e reduz o uso da largura de banda. (A compactação de análise nos dispositivos Linux não é usada.)

Criptografia da análise

As análises de inventário nos dispositivos Windows são criptografadas (apenas as análises TCP/IP). Você pode desativar a criptografia de análise de inventário mudando um parâmetro em Configurar serviços.

1. No servidor núcleo, clique em **Iniciar > Todos os programas > LANDesk > Configurar serviços LANDesk**
2. Clique na guia **Inventário** e clique em **Configurações avançadas**.
3. Clique em **Desabilitar criptografia**. Digite **1** na caixa **Valor**.
4. Clique em **Definir**, em seguida clique em **OK**.
5. Clique em **OK,** e depois em **Sim** ao ser avisado para reiniciar o serviço.

Visualização dos dados de inventário

Quando um dispositivo é analisado pela análise de inventário, é possível ver suas informações de sistema das formas a seguir:

- Como ver o resumo de inventário
- Como ver o inventário completo
- Como ver propriedades de atributos
- Como ver as informações do sistema

Também é possível ver os dados de inventário em relatórios que você gera.

Como abrir o resumo de inventário no console de inventário de tempo real

O resumo de inventário é encontrado na página de **Resumo** no console de informações do servidor e fornece uma vista rápida da configuração básica de SO e das informações de sistema do dispositivo.

NOTA: Se você adicionou um dispositivo ao banco de dados núcleo usando a ferramenta de descoberta, seus dados de inventário ainda não terão sido analisados no banco de dados núcleo. É preciso executar uma análise de inventário no servidor para que o recurso Resumo de inventário seja completado com êxito.

Para ver o resumo de inventário

1. No tela de rede do Console de gerenciamento da LANDesk, em um grupo **Dispositivos**, clique com o botão direito em um dispositivo e selecione **Inventário e monitoração em tempo real**.
2. Na caixa de ferramentas, clique em Informações do Sistema **> Resumo do sistema** .

Dados do resumo

Essas informações aparecem quando você vê o resumo de inventário de um dispositivo gerenciado.

- **Funcionamento:** O estado do funcionamento atual do dispositivo.
- **Tipo:** O tipo do dispositivo.
- **Fabricante:** O fabricante do dispositivo.
- **Modelo:** O tipo do modelo do dispositivo.
- **Versão do BIOS:** A versão do BIOS da ROM.
- **Sistema operacional:** SO Windows ou Linux em execução no dispositivo.
- **Versão do SO:** O número da versão do SO executando no dispositivo.
- **CPU:** O tipo de processador ou processadores em execução no dispositivo.
- **Analisador de vulnerabilidades:** A versão do agente instalado.
- **Controle remoto:** A versão do agente instalado.
- **Distribuição de software:** A versão do agente instalado.
- **Analisador de inventário:** A versão do agente instalado.
- **Monitoração:** A versão do analisador de monitoração instalado.
- **Última inicialização:** A data e o horário da última vez em que o dispositivo foi reinicializado.

- **Utilização da CPU:** Porcentagem atual em uso do processador.
- **Memória física usada:** Quantidade de RAM disponível no dispositivo.
- **Memória virtual usada:** Quantidade de memória disponível para o dispositivo, incluindo a RAM e a memória do arquivo de troca.
- **Espaço usado da unidade:** Porcentagem de espaço da unidade em uso no momento. Se houver mais de uma unidade de disco, todas as unidades serão mostradas.

Os dispositivos que são habilitados para IPMI IPMI visualizar dados específicos adicionais. Dispositivos Linux também mostram informações semelhantes na tela do **Resumo**.

Como ver o inventário completo

Um inventário completo fornece uma listagem completa dos componentes de hardware e software detalhados de um dispositivo. A lista contém objetos e atributos de objetos.

Para ver um inventário completo

1. Na tela de rede do Console de gerenciamento da LANDesk, em um grupo **Dispositivos**, clique duas vezes em um dispositivo.
2. Na ferramenta **Meus dispositivos,** do console Web, selecione um grupo (como Meus dispositivos) e clique em um dispositivo. No painel da ação, clique na **guia Propriedades** e, em seguida, clique em **inventário da vista** .

Como ver propriedades de atributos

É possível visualizar as propriedades de atributo dos objetos Inventário de um dispositivo na listagem de inventários. As propriedades de atributo informam as características e os valores de um objeto do inventário. Também é possível criar novos atributos personalizados e editar os atributos definidos pelo usuário.

Para ver as propriedades de um atributo

1. Na lista completa de inventário, clique no atributo no painel esquerdo. Pode ser necessário para expandir os itens para encontrar o atributo que você deseja.
2. Para imprimir a informação, utilize a função **Imprimir** do seu navegador.

Como ver as informações do sistema

Do tempo real Inventário e monitoramento console, você pode visualizar e modificar as informações de sistema do dispositivo. As informações do **Hardware** , **Registros** , **Software** e **outras** categorias é quer dados armazenados ou dados em tempo real. Quando clica em um link de informações, você pode ver informações detalhadas sobre o componente selecionado e, quando apropriado, definir limites e inserir informações.

1. Em **Todos os dispositivos**, no modo de exibição do console Web, clique duas vezes em um dispositivo.
2. Na caixa de ferramentas, clique em **Informações do sistema**.
3. Expanda o grupo e clique no link das informações que deseja ver.

Configurando links do banco de dados de rollup [console Web]

Esta seção descreve a maneira de configurar os links de banco de dados no núcleo de rollup. As situações são:

- Rollup de Oracle para Oracle
- Rollup de SQL Server para SQL Server

A pessoa que faz a configuração deve também ter acesso a todos os DBMSs usados pela LANDesk e precisam ter permissão de segurança para criar links de banco de dados e executar as etapas de configuração no nível de servidor de DBMS.

Rollup de Oracle para Oracle

Configuração do banco de dados Oracle

O arquivo TNSNames.ora no servidor de banco de dados onde o seu banco de dados de rollup existe deve conter uma entrada para o seu banco de dados do servidor núcleo.

1. No caso do banco de dados Oracle, dentro do Console do Enterprise Manager, conecte ao seu banco de dados. Expanda **Distribuído**.
2. No menu de atalho do item **Links de banco de dados** clique em **Criar**.
3. No campo **Nome**, digite um nome para o link de banco de dados.
   Observação: se o banco de dados AR estiver usando Oracle9i, o nome do link pode ser qualquer nome que já não esteja em uso ou reservado. A instalação solicitará essas informações.
4. Selecione **Usuário fixado** e digite o nome de usuário e a senha para o banco de dados do servidor núcleo.
5. No campo **Nome do serviço**, digite a entrada TNSNames.ora (por exemplo, NetAlias) que se refere ao seu banco de dados do servidor núcleo.
6. Clique em **Criar**.
7. Clique duas vezes no seu link recém-criado e clique em **Testar**. Uma mensagem indicando que o seu link está ativo deverá ser exibida. Você também pode testar seu link acessando o banco de dados de rollup e emitindo o seguinte comando:

   Select count(*) from computer@linkname;
   Se o retorno for uma contagem de dispositivos no banco de dados de produção do servidor núcleo, isso significa que o link está configurado corretamente.

Rollup de SQL Server para SQL Server

Configuração do banco de dados SQL Server

1. Abra o SQL Server Management Studio.
2. Expanda o seu servidor e, em seguida, **Objetos de Servidor**.
3. No menu de atalho do item **Servidores vinculados**, clique em **Novo servidor vinculado**.
4. Na guia **Geral**, siga as etapas de 5 a 11:
5. **Servidor vinculado:** digite um nome exclusivo para esse link de banco de dados (por exemplo, Link LDMS core server1).
6. Escolha **Outra fonte de dados.**
7. Selecione **Microsoft OLE DB Provider para SQL Server**.
8. **Nome do produto**: insira o LDMS.
9. **Fonte de dados:** digite o nome do servidor do banco de dados contendo o banco de dados núcleo.

10. **String do provedor:** insira a string do provedor. Por exemplo:

    SQL Server
    provider=SQLOLEDB.1;user id=<Usuário do banco de dados do servidor núcleo>
    *** A parte do id de usuário da string do provedor é necessária na string de conexão a outro banco de dados SQL Server. ***

11. **Catálogo:** digite o nome físico do banco de dados do seu servidor núcleo (por exemplo, lddb).
12. Na guia **Segurança**, selecione **Ser feito usando este contexto de segurança** e digite o nome de usuário e a senha para o banco de dados do servidor núcleo. Em seguida, clique em **OK**.
13. Clique em **Nova consulta** e digite o seguinte comando:

    Selecione contagem(*) de [Nome do link].[nome do banco de dados].[Nome do dono da mesa].Computador

    Usando os valores acima, esta consulta será exibida como:

    Selecione contagem(*) em [LDMS Core Server1 Link].[lddb].[dbo].Computer
    Se a contagem correta voltar, o seu link está configurado corretamente.

Suporte a multi-núcleos [console Web]

Para poder utilizar mais de um núcleo, devem ser satisfeitas as seguintes condições:

- Os núcleos devem ser parte do mesmo domínio.
- A conta de administrador de domínio devem ser adicionados ao grupo de usuários locais do LANDesk Management Suite em ambos os núcleos.
- A identidade do aplicativo COM+ da LANDesk nos serviços de componente deve ser definida como o administrador do domínio Isso é descrito na seção a seguir.
- O arquivo core.asp deve ser editado de forma a incluir o segundo núcleo. O arquivo core.asp está na pasta \inetpub\wwwroot\LANDesk\LDMS\xml. Ao acessar inicialmente o console Web em um navegador, você vai ver uma lista pendente que inclui os servidores definidos no core.asp. Adicione os dispositivos que desejar e clique em **Conectar**.

Abaixo está um exemplo do core.asp que inclui vários servidores.

```
<?xml version="1.0" ?>
<core>
<cores>
<item name="Core_Host_Name_1" rollup="0"/>
<item name="Core_Host_Name_2" rollup="0"/>
<item name="Rollup_Core_Host_Name_3" rollup="1"/>
</cores>
</core>
```

Para acessar um núcleo em um ambiente de múltiplos núcleos

1. Abrir o Web ConsoleManagement Suite.
2. Na lista **Selecionar um núcleo**, selecione o núcleo que deseja acessar e clique em **Conectar**. Digite o nome de usuário e a senha.

Notas

- Para completar com êxito a configuração do cliente, use o URL correto para o núcleo. Caso contrário, a configuração não funcionará.
- Você pode achar que é útil adicionar entradas para cada servidor do núcleo nos favoritos do seu navegador. Isso facilita a mudança entre os núcleos.

Configuração das credenciais do servidor COM+

Ao usar um servidor de Web console diferente do núcleo ou, se quiser usar grupos de domínio dentro do grupo LANDesk Management Suite no servidor núcleo, é necessário fazer algumas configurações adicionais de servidor a serem feitas para a autenticação do Management Suite funcionar corretamente. Os servidores de Web console devem obter as informações de conexão do banco de dados e as informações do usuário do servidor núcleo, entretanto esses servidores usam credenciais personificadas de Web no IIS, por isso eles não podem comunicar-se com o servidor núcleo diretamente.

Para resolver esse problema, o servidor de Web console e o servidor núcleo usam um aplicativo COM+ para comunicar-se via HTTPS, o que permite ao servidor de Web console obter informações do banco de dados e do usuário. É necessário configurar esse aplicativo COM+ no servidor Web console para usar uma conta com os direitos necessários como, por exemplo, uma conta de administrador de domínio. A conta que for fornecida precisa estar no grupo LANDesk Management Suite no servidor núcleo (isso permite o acesso às informações de conexão do banco de dados do servidor núcleo) e deve ter direitos para enumerar membros de domínio Windows.

Se estiver usando grupos de domínio dentro do grupo LANDesk Management Suite do servidor núcleo, o Management Suite também precisa poder enumerar os membros do domínio also Windows. Nesse caso, é necessário também fornecer uma conta para o aplicativo LANDesk1 COM+ do servidor núcleo.

Para configurar o aplicativo LANDesk1 COM+ em um núcleo ou servidor de Web console remoto

1. Vá para o servidor de Web ou o servidor núcleo que deseja configurar.
2. Nas Ferramentas administrativas do Painel de controle do Windows, abra **Serviços de componente**.
3. Clique em **Serviços de componente > Computadores Meu computador > Aplicativos COM+.**
4. No menu de atalho do aplicativo **LANDesk1** COM+ e selecione **Propriedades**.
5. Na guia **Identidade**, digite as credenciais que quer usar.
6. Clique em **OK**.

Gerenciador de inventário

Gerenciador de inventário LANDesk

O LANDesk Gerenciador de inventário é uma versão do LANDesk Management Suite 9 que contém apenas os seguintes recursos relacionados a inventário:

- Análise de inventário e recursos de console relacionados a inventário
- Formulários de dados personalizados
- Monitoramento de licenças de software
- Descoberta de dispositivos não gerenciados
- Relatórios para os recursos acima

A instalação do Gerenciador de inventário em um servidor núcleo contém todos os componentes do Management Suite 9, mas quando você ativa um servidor núcleo com uma conta que é licenciada para o Gerenciador de inventário, os recursos que não pertencem ao Inventory Manager não são aplicáveis ou não são visíveis no Management Suite nem nos Web consoles.

Se estiver usando o Gerenciador de inventário, consulte as seções que correspondem à lista de recursos acima. Em geral, você reconhece as informações não aplicáveis em cada capítulo, pois essas seções referem-se a recursos do Management Suite como, por exemplo, distribuição de software e controle remoto, as quais não são parte do Gerenciador de inventário.

Gerenciamento de hardwares HP

Visão geral da LANDesk Management Suite com Gerenciamento de hardwares e softwares HP

A ferramenta éLANDesk Management Suite plus HP Hardware and Software Management uma solução integrada de parceiro para seu ouLANDesk® Management SuiteLANDesk Security Suite ambiente de rede. O LANDesk plus HP Management permite que você proteja e gerencie seus dispositivos HP e dispositivos periféricos (RPOS) remotamente, a partir de um único console.

Esta solução combina os recursos de gerenciamento da HP com as ferramentas poderosas do LANDesk Management Suite que permite que os administradores da LANDesk verifiquem de forma fácil e eficaz dispositivos gerenciados HP, visualizem dados de componentes de inventário (hardware e software), executar consultas, implementem e instalem as últimas atualizações da HP, configurem alertas de funcionamento e gerem relatórios.

Essa funcionalidade integrada, em conjunto com as ferramentas de alertas e relatórios LANDesk, ajuda os administradores da LANDesk a identificar e lidar com o uso de dispositivos periféricos do ponto de venda de varejo, excessos e erros de hardware, consumo e desempenho de energia, funcionamento da bateria, status de conectividade da placa de rede HP, questões de manutenção, ausência de dispositivos e assim por diante.

O que há de novo no lançamento da atualização da HP 1.4

A HP 1.4 liberação de adiciona suporte para *HP Thin Client Management* . Várias ferramentas úteis do LANDesk Management Suite e do Security Suite estão disponíveis, o que permite descobrir, configurar, gerenciar e proteger dispositivos HP Thin Client em sua rede.

A versão LANDesk Management Suite9.5 oferece suporte às seguintes plataformas HP Thin Client:

- Windows Embedded Standard 7 Enterprise (WES7)
- Windows Embedded Standard 09 Enterprise (WES09)
- HP ThinPro Linux Ubuntu

IMPORTANTE: O LDMS 9.5 inclui a mais recente funcionalidade do Gerenciamento de hardwares e softwares da HP
Os novos recursos da versão HP 1.4 — ferramentas de Gerenciamento do HP Thin Client — serão incluídos por padrão com o lançamento da versão 9.5 da LANDesk Management Suite. Em outras palavras, ao fazer o download e a instalação da LDMS 9.5, você receberá todas as funcionalidades anteriores do HP 1.2 e 1.3. NÃO há nenhuma exigência para uma instalação separada dos lançamentos anteriores da HP.

A LANDesk com Gerenciamento do HP Thin Client oferece as seguintes ferramentas e recursos da LANDesk:

- Descoberta de dispositivos não gerenciados (UDD)
- Configuração de agentes
- Provisionamento de captura de imagem e implantação
- Gerenciamento do filtro de gravação (SOMENTE plataformas do WES)

- Distribuição do software
- Gerenciamento de patches
- Controle remoto
- Exibição Inventário

Para obter mais informações sobre o Gerenciamento do HP Thin Client, consulte "Gerenciamento de dispositivos HP Thin Client a partir do console LANDesk" na página 984

O que há de novo no lançamento da atualização da HP 1.3

O lançamento HP 1.3 adiciona recursos de gerenciamento de *softwares* da HP. O produto agora é chamado **LANDesk Management Suite com Gerenciamento de hardwares e softwares HP**.

Agora, os administradores de sistema podem utilizar ferramentas integradas da HP para monitorar e gerenciar os recursos adicionais de software específicos dos dispositivos HP gerenciados.

As ferramentas de gerenciamento HP adicionadas recentemente incluem:

- **Assistente de energia da HP —** Essa ferramenta permite monitorar e gerenciar o uso de energia em dispositivos HP. Utilize as configurações personalizadas de energia e implemente-as como dispositivos de destino HP, com a finalidade de otimizar o consumo e o desempenho de energia. Os dados do Assistente de energia da HP estão disponíveis no inventário do dispositivo e em relatórios predefinidos.
- **Verificador de bateria da HP —** Essa ferramenta verifica automaticamente o dispositivo HP gerenciado e permite acompanhar o funcionamento da bateria do dispositivo. Os dados do Verificador de bateria da HP estão disponíveis no inventário do dispositivo e em relatórios.
- **Gerenciador de conexões da HP —** Essa ferramenta verifica automaticamente os dispositivos gerenciados HP para comparar o status da placa de rede compatível com produtos HP e relata essas informações para o banco de dados do núcleo. É possível utilizar essas informações para ativar uma placa de rede, o que permite controlar e gerenciar a conectividade e atividade da rede (Internet).
- **Diretivas de Software da HP —** Utilize esta nova ferramenta (disponível na janela da ferramenta **Configurações de segurança**) para criar políticas personalizadas com base nas configurações do Assistente de energia da HP que podem ser implementadas para os dispositivos gerenciados da HP por meio da tarefa Alterar configurações e da ferramenta Tarefas agendadas.

É possível visualizar esses novos dados no inventário do dispositivo, no nó do componente **Hewlett-Packard**.

Além disso, os novos relatórios a seguir foram adicionados à ferramenta Relatórios da LANDesk:

- Verificação das condições de funcionamento da bateria da HP
- Informações do recurso do cartão de banda larga móvel da HP
- Consumo de energia do assistente de energia da HP
- Consumo de energia do Assistente de energia da HP em comparação com o dia da semana

Para obter mais informações sobre o gerenciamento do cliente HP, consulte Gerenciamento de dispositivos HP a partir do console LANDesk.

Recursos anteriores (introduzidos no lançamento inicial da versão HP 1.2)

A versão HP 1.2 é o lançamento inicial da ferramenta **LANDesk Management Suite com Gerenciamento de hardwares HP**. Com essa solução integrada, os administradores de sistema podem:

- Acessar ferramentas integradas de gerenciamento do dispositivo HP no console LANDesk
- Configurar dispositivos HP para gerenciamento (exame, inventário em tempo real, monitoramento, alertas e relatórios)
- Executar análises de inventário em dispositivos HP
- Exibir o inventário de dispositivos HP (incluindo dispositivos para pontos-de-venda de varejo)
- Exibir em tempo real o inventário e monitoramento de dispositivos HP
- Executar consultas usando dados de inventário de componentes HP específicos
- Configurar e distribuir configurações de BIOS da HP para dispositivos HP
- Configurar e distribuir as configurações do chip de segurança TPM (Trusted Platform Module) nos dispositivos HP selecionados
- Alterar/atualizar as configurações de BIOS e TPM com a ferramenta Tarefas agendadas
- Distribuir e instalar as últimas atualizações da HP (incluindo atualizações de hardware e firmware HP)
- Configurar alertas de saúde para eventos, erros, limites de uso e outros atributos de dispositivos gerenciados HP e periféricos de pontos-de-venda de varejo
- Gerar relatórios, incluindo de inventário padrão e BIOS, além dos relatórios predefinidos sobre dispositivos HP

Dispositivos de ponto de venda de varejo (RPOS)

Os dispositivos de ponto de venda de varejo incluem:

- HP AP5000
- HP Cash Drawer
- Impressora híbrida da HP com MICR
- Leitor de código de barras com captura de imagem da HP
- Teclado HP
- Teclado HP com MSR
- Leitor de código de barras a laser da HP
- Mini MSR (Leitor de banda magnética) da HP
- Visor de linha de torre HP
- HP RP5800
- Impressora térmica de recibos da HP
- mais...

Introdução

Para utilizar as ferramentas do LANDesk Management Suite com Gerenciamento de hardwares e softwares HP você deve primeiro instalar o pacote de softwares da HP (SOMENTE nos servidores núcleo da versão 9.0 do LDMS) e configurar os dispositivos HP com os agentes LANDesk necessários.

Para iniciar o processo, visite "Pré-requisitos de instalação" na página 944.

Onde obter mais informações

Para obter mais informações sobre como utilizar as ferramentas e recursos LANDesk Management Suite, você pode consultar os tópicos de ajuda da LANDesk Management Suite.

Navegue pelo tópicos de ajuda do LANDesk Management Suite na Central de ajuda LANDesk ou execute execute uma busca usando uma palavra-chave ou frase para encontrar a informação que você deseja.

Para obter informações detalhadas sobre a instalação e configuração do servidor núcleo LANDesk, consulte os documentos do *Método mais conhecido de instalação e distribuição*, disponíveis no portal da comunidade de usuários da LANDesk.

NOTA: A Comunidade de usuários da LANDesk
Além disso, a Comunidade de usuários LANDesk tem fóruns de usuários e os melhores métodos conhecidos para todos os produtos e tecnologias LANDesk. Para acessar esse recurso valioso, visite: http://community.landesk.com

Pré-requisitos de instalação

Esta seção descreve os requisitos de hardware e software para a instalação do LANDesk plus HP Management HP e dos dispositivos HP que você deseja gerenciar por meio do console LANDesk com as ferramentas integradas da HP.

Você deve atender aos seguintes pré-requisitos para instalar, configurar e usar a LANDesk Management Suite com as ferramentas do LANDesk Management Suite plus HP Hardware and Software Management em seu ambiente de rede.

Pré-requisitos do servidor núcleo LANDesk

- **IMPORTANTE:** Windows Server 2008 R2 x64 como servidor núcleo
- Servidor núcleo LDMS 9.0 instalado, com a versão SP3 instalada (pode ser baixado da Comunidade de usuários da LANDesk)

NOTA: Documentos de instalação e configuração na comunidade de usuários da LANDesk
Se o servidor núcleo da LANDesk não estiver instalado, consulte a seção de instalação do seguinte documento na Comunidade de usuários da LANDesk: Community Document 7423.

Se você estiver executando um **servidor núcleo LDMS 9.0** — é necessário instalar o software de integração da HP. Para obter mais informações, consulte "Instale software de Gerenciamento de hardwares e softwares da HP" na página 945.

Se você estiver executando um **servidor núcleo LDMS 9.5** — não é necessário instalar o software de integração da HP. Agora você está pronto para configurar clientes HP, HP Thin Client e gerenciá-los por meio do console LANDesk. Para obter mais informações, consulte "Configure os dispositivos da HP para tarefas de Gerenciamento da LANDesk" na página 946.

Pré-requisitos do cliente HP

Os dispositivos de cliente padrão da HP devem ter:

- os sistemas operacionais Windows XP, Windows Vista (32 bits, 64 bits) ou Windows 7 (32 bits, 64 bits) em execução. **(IMPORTANTE:** A ferramenta de configurações do chip de segurança HP TPM NÃO é compatível com o sistema operacional Windows XP.)

- Agente LANDesk padrão instalado (configurado para alertas e inventário e monitoramento em tempo real). Para obter mais informações, consulte "Configure os dispositivos da HP para tarefas de Gerenciamento da LANDesk" na página 946.
- CMI providers instalados. Esta atualização HP leva o nome *"HP Client Management Interface Software Providers"* (**OBS.:** Caso ainda o arquivo ainda não esteja instalado, é possível baixá-lo em instalá-lo no site da HP)
- Fornecedores para pontos-de-venda de varejo (RPOS) instalados. Esta atualização HP leva o nome *"HP Retail Windows Management Instrumentation (WMI) Provider"* (**OBS.:** Caso ainda o arquivo ainda não esteja instalado, é possível baixá-lo em instalá-lo no site da HP)

NOTA: Baixe e instale os provedores CMI e RPOs por meio do console LANDesk
Se ainda não estiverem instalados, é possível baixar e instalar remotamente os provedores CMI e RPOs em dispositivos HP por meio do console LANDesk. Use a ferramenta de **Patch e conformidade** da LANDesk Management Suite ou a ferramenta **Software Distribution**.

Agora é possível verificar o dispositivo “gerenciado” HP, visualizar o inventário de dispositivos, configurar a BIOS e as configurações de chip TPM, criar e implementar políticas de software HP com a configuração do Assistente de energia da HP, utilizar as ferramentas Verificação de bateria da HP e Gerenciador de conexões da HP etc. Para obter mais informações, consulte Gerenciamento de dispositivos HP a partir do console LANDesk.

Pré-requisitos do HP Thin Client

Os dispositivos HP Thin Client devem ter:

- Os sistemas operacionais Windows Embedded Standard 7 Enterprise (WES7), Windows Embedded Standard 09 (Enterprise WES09) ou HP ThinPro (Ubuntu) em execução no dispositivo.
  (IMPORTANTE: No momento, o HP ThinPro Ubuntu suporta APENAS o serviço de inventário do agente LANDesk padrão.
- Agente LANDesk padrão instalado. Para obter mais informações, consulte "Configurar dispositivos Windows Embedded Standard (WES) HP Thin Client" na página 949 e "Configurar os dispositivos HP ThinPro Linux" na página 952.

Após atender a esses pré-requisitos do dispositivo HP, é possível fazer escolher uma das seguintes opções:

- Se você estiver executando um **servidor núcleo LDMS 9.0** — é necessário instalar o software de integração da HP. Para obter mais informações, consulte "Instale software de Gerenciamento de hardwares e softwares da HP" na página 945.
- Se você estiver executando um **servidor núcleo LDMS 9.5** — não é necessário instalar o software da HP. Agora você está pronto para configurar clientes HP, HP Thin Client e gerenciá-los por meio do console LANDesk. Para obter mais informações, consulte "Configure os dispositivos da HP para tarefas de Gerenciamento da LANDesk" na página 946.

Instale software de Gerenciamento de hardwares e softwares da HP

Este tópico fornece instruções passo a passo para instalar o LANDesk Management Suite com Gerenciamento de hardwares e softwares HP em servidor núcleo.

IMPORTANTE: A instalação necessária somente para LDMS 9.0 / ambiente de servidor do núcleo
este procedimento só é aplicável se você estiver executando a versãoLANDesk Management Suite 9.0

(com o SP3 instalado). Se você estiver usando LDMS 9.0 , você deve executar os passos de instalação abaixo. No entanto, se você atualizou para o LANDesk Management Suite versão 9.5, você pode ignorar este procedimento porque todas as ferramentas de gerenciamento da HP são integradas.

Instale o software de Gerenciamento da HP no servidor núcleo do LDMS

IMPORTANTE: Conformidade com os prerrequisitos de instalação
Certifique-se de que você atende todos os requisitos desta instalação. Para obter mais detalhes, consulte "Pré-requisitos de instalação" na página 944 .

Conclua a seguinte lista de passos para instalar o software da HP.

Para instalar o software da HP

1. Sobre o servidor núcleo, veja o DOC-24825 da comunidade de usuários da LANDesk, "Como instalar o LANDesk com Gerenciamento da HP" e faça o download do arquivo "LD90-SP3-HP-Release-1.3.exe".
2. Execute o arquivo do download. Extrai a: C: \LD90-HP (ou você pode escolher outro diretório).
3. Abra a pasta extraída.
4. Abra o "LD90-SP3-HP-Release-1.3" diretório.
5. Extrair o "LD90-SP3-HP-Release-1.3 .zip" arquivo.
6. Abra a pasta extraída.
7. Executar o Setup.program de exe.
8. Siga os avisos.
9. Clique em **Instalar** na página de instalação. O assistente de Instalação exibe o progresso e status da instalação.
10. Na página Concluído, clique em **Terminar**.
11. Quando as mensagens Concluído / Instalação bem-sucedida forem exibidas, clique em **Fechar**.

O que vem a seguir?

O próximo passo é configurar seus dispositivos HP com o Agente LANDesk padrão. Para obter mais informações, consulte "Configure os dispositivos da HP para tarefas de Gerenciamento da LANDesk" na página 946.

Configure os dispositivos da HP para tarefas de Gerenciamento da LANDesk

Antes de gerenciar seus dispositivos HP, você deve configurá-los com o agente padrão da LANDesk (CBA ou Common Base Agent). Isso os torna dispositivos gerenciados no banco de dados do núcleo da LANDesk e permite que as diversas tarefas de gerenciamento sejam realizadas — incluindo as tarefas de Gerenciamento de hardwares e softwares da HP— através do console LANDesk.

HP dispositivos adicionais que podem ser configuradas

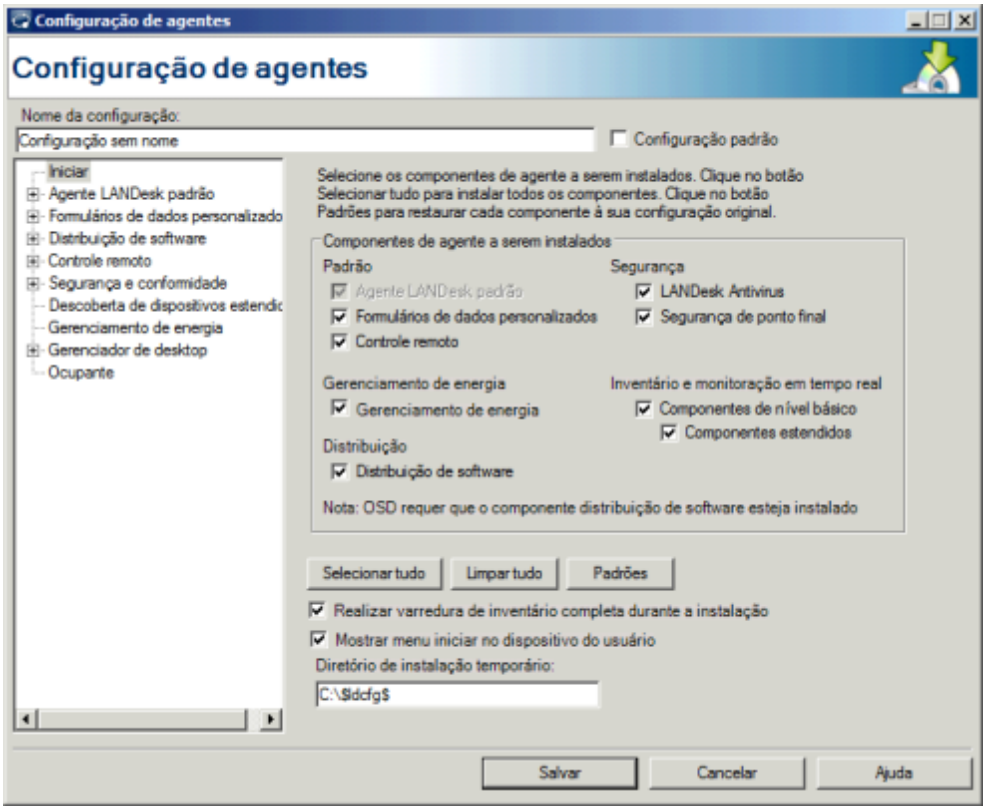
Você também pode configurar (como dispositivos gerenciados) estes tipos de plataformas HP e gerenciá-los com as ferramentas da LANDesk.

- Windows Embedded Standard 7 Enterprise (WES7) — Para obter mais informações, consulte "Configurar dispositivos Windows Embedded Standard (WES) HP Thin Client" na página 949.
- Windows Embedded Standard 09 Enterprise (WES9) — Para obter mais informações, consulte "Configurar dispositivos Windows Embedded Standard (WES) HP Thin Client" na página 949.
- HP ThinPro Linux Ubuntu — Para obter mais informações, veja "Configurar os dispositivos HP ThinPro Linux" na página 952.

Distribuir o agente LANDesk para dispositivos HP

Para distribuir o agente LANDesk

1. A partir da máquina HP, mapeie um drive no servidor núcleo, vá até a pasta LDLogon e execute o wscfg32.exe. (Ou, para distribuir uma configuração de agente a partir do console através de uma tarefa agendada, clique em **Ferramentas > Configuração > Configuração de agente** para abrir a caixa de diálogo Configuração de agente.)
2. Clique com o botão direito em **Minhas configurações** e em **Nova configuração do agente Windows**.
3. Na página **Iniciar**, insira um nome único para a configuração.
4. Na **Página inicial**, certifique-se que em **Inventário e monitoração em tempo real** as opções **Componentes da linha de base** e **Componentes estendidos** estão selecionadas. (**NOTA:** O recurso LANDesk Alerting é habilitado por padrão com om agente LANDesk padrão.)



5. Selecione cada página e especifique as opções que você deseja aplicar a esta configuração que serão implantados dispositivos de destino (clique em Ajuda sobre qualquer página para obter informações detalhadas).
6. Clique em **Instalar**.

   OU

   Se você estiver distribuindo a configuração do agente *a partir do* console da LANDesk para os dispositivos alvo, clique em **Salvar** para adicionar a tarefa à janela da ferramenta Tarefas agendadas, onde você poderá configurar uma tarefa para distribuir a configuração de agente aos dispositivos HP desejados.

Use o LANDesk Management Suite para controlar seus dispositivos HP

Após configurar um dispositivo HP com o agente LANDesk, ele se torna um dispositivo "gerenciado" no ambiente de rede da LANDesk.

Na tela de rede

Na Tela de rede do console da LANDesk, clique com o botão direito em um dispositivo gerenciado da HP para acessar o menu de atalho onde você poderá:

- Executar uma análise de inventário
- Veja os dados do inventário do dispositivo da HP (configurações do BIOS, do chip de segurança, Assistente de energia da HP, Verificador de bateria da HP, Gerenciador de conexões da HP, além dos dados de periféricos de RPOS)

No console

No console, você também poderá:

- Acessar as novas ferramentas integradas de Gerenciamento de hardwares da HP no console da LANDesk
- Configure (altere/atualize) as configurações do BIOS da HP e do chip TPM
- Configure (mude/atualize) os parâmetros do assistente de energia da HP
- Crie e execute consultas com base nos dados de inventário de dispositivos específicos da HP (componentes e atributos)
- Configure alertas com base nos dados de inventário de dispositivos da HP
- Gere relatórios com base nos dados de inventário de dispositivos da HP

Para obter informações detalhadas e instruções passo-a-passo sobre todas essas tarefas, vá para Gerenciamento de dispositivos HP a partir do console LANDesk.

Tópicos relacionados

Gerenciamento de dispositivos HP a partir do console LANDesk

Configurar dispositivos Windows Embedded Standard (WES) HP Thin Client

Antes de gerenciar seus dispositivos HP Thin, você deve configurá-los com o agente LANDesk padrão (CBA ou Common Base Agent (Agente de Base Comum)). Isso os torna dispositivos gerenciados no banco de dados do núcleo LANDesk e permite que as diversas tarefas de gerenciamento sejam realizadas — incluindo as tarefas de Gerenciamento de hardwares e softwares de parceiros da LANDesk — por meio do console LANDesk.

A versão LANDesk Management Suite do 9.5 oferece suporte às seguintes plataformas HP Thin Client WES:

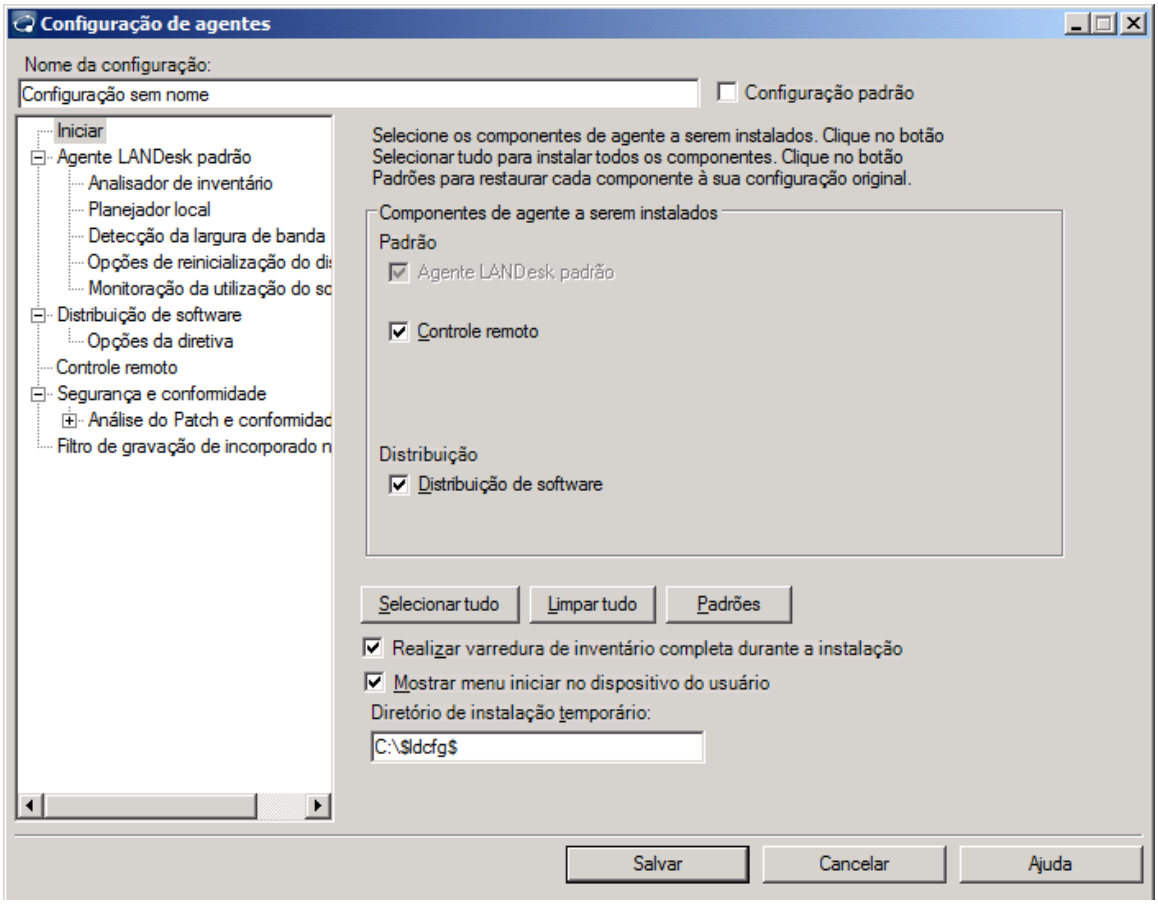
- Windows Embedded Standard 7 Enterprise (WES7)
- Windows Embedded Standard 09 Enterprise (WES09)

Distribuir o agente LANDesk em dispositivos WES HP Thin

Para distribuir o agente LANDesk

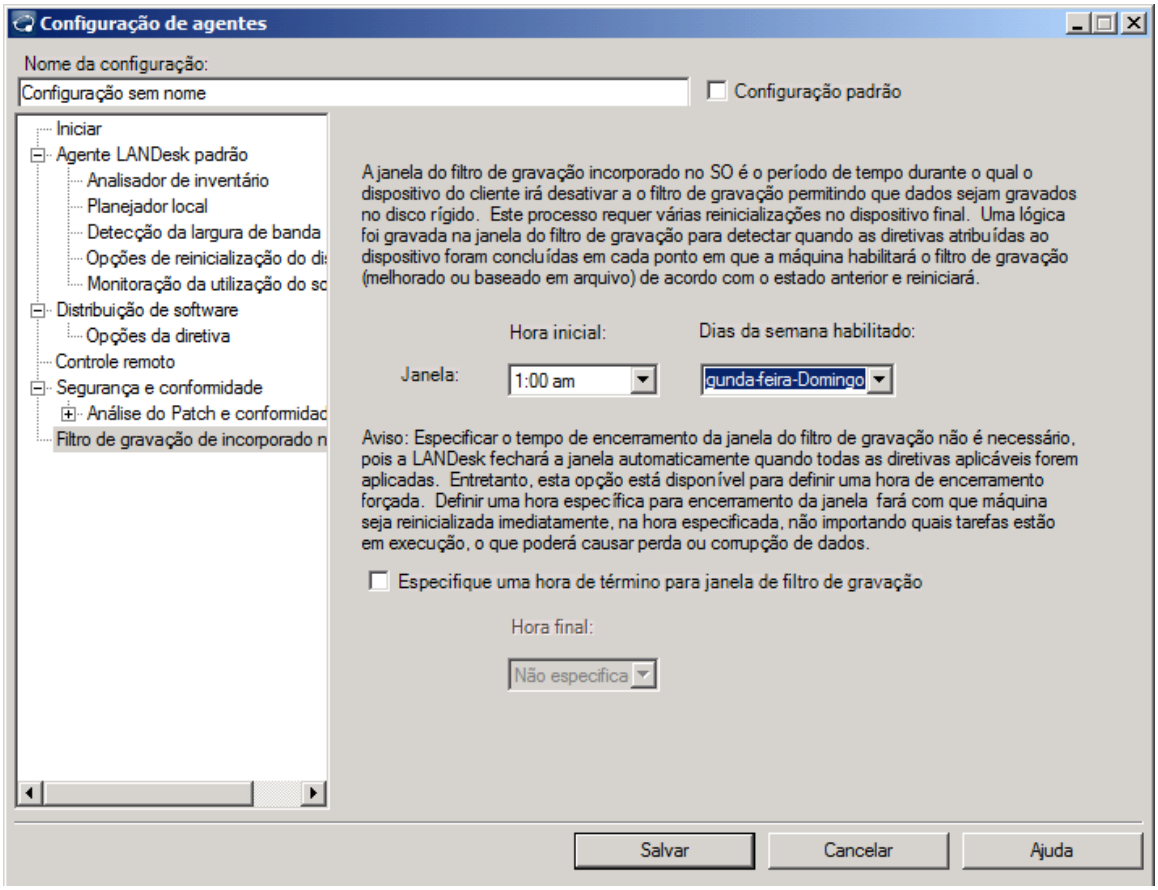
1. A partir do console, clique em **Ferramentas > Configuração > Configuração de agente** para abrir a caixa de diálogo Configuração de agente.
2. Clique com o botão direito em **Minha Configuração do novo agente padrão incorporado do Windows**.
3. Na página **Iniciar**, insira um nome único para a configuração.

4. A caixa de diálogo de Configuração de Agente é semelhante à configuração normal de agente de Windows opções e controles. Selecione cada página e especifique as opções que você deseja aplicar a esta configuração que serão implantados dispositivos de destino (clique em Ajuda sobre qualquer página para obter informações detalhadas).



5. Uma característica específica de gerenciamento do Thin Client HP WES é a opção do filtro de gravação incorporado ao SO. Clique na página do **Filtro de gravação de SO incorporado** para configurar um período de tempo durante o qual o "filtro de gravação" está inativado no dispositivo gerenciado para que o Administrador da LANDesk possa executar as tarefas de manutenção na máquina. (**NOTA:** A maneira como isso funciona é que o filtro de gravação no disco rígido do dispositivo de destino estiver desativado, o dispositivo é reiniciado, e no final do período de tempo especificado, ou quando todas as tarefas e processos inventariadas são completos, o filtro de gravação é novamente ligado, o dispositivo é reiniciado novamente.) Você pode configurar a Hora de início, dias da semana durante o qual as janelas de manutenção são permitidas e a Hora de término do filtro de gravação.

   Para obter mais informações, consulte "Distribuindo o filtro escritura para dispositivos Windows Embedded Standard." na página 133.


Configuração de agentes
Nome da configuração:
Configuração sem nome
Configuração padrão
Iniciar
Agente LANDesk padrão
Analisador de inventário
Planejador local
Detecção da largura de banda
Opções de reinicialização do di
Monitoração da utilização do sc
Distribuição de software
Opções da diretiva
Controle remoto
Segurança e conformidade
Análise do Patch e conformidad
Filtro de gravação de incorporado n
A janela do filtro de gravação incorporado no SO é o período de tempo durante o qual o dispositivo do cliente irá desativar a o filtro de gravação permitindo que dados sejam gravados no disco rígido. Este processo requer várias reinicializações no dispositivo final. Uma lógica foi gravada na janela do filtro de gravação para detectar quando as diretivas atribuídas ao dispositivo foram concluídas em cada ponto em que a máquina habilitará o filtro de gravação (melhorado ou baseado em arquivo) de acordo com o estado anterior e reiniciará.
Hora inicial:
Dias da semana habilitado:
Janela:
1:00 am
gunda-feira-Domingo
Aviso: Especificar o tempo de encerramento da janela do filtro de gravação não é necessário, pois a LANDesk fechará a janela automaticamente quando todas as diretivas aplicáveis forem aplicadas. Entretanto, esta opção está disponível para definir uma hora de encerramento forçada. Definir uma hora específica para encerramento da janela fará com que máquina seja reinicializada imediatamente, na hora especificada, não importando quais tarefas estão em execução, o que poderá causar perda ou corrupção de dados.
Especifique uma hora de término para janela de filtro de gravação
Hora final:
Não especifica
Salvar
Cancelar
Ajuda

CUIDADO: Se você definir uma hora de término específico para o filtro de gravação ser habilitado e para diretivas e processos serem executados e todos os processos incompletos até esse tempo, lembre-se que perda de dados ou corrupção podem ocorrer. Portanto, você precisa medir com exatidão e determinar a quantidade de tempo solicitado para completar todas as diretivas aplicadas e tarefas. Ou, então NÃo defina uma hora de término.

6. Clique em **Salvar**. Isso adiciona a tarefa para a ferramenta janela das Tarefas Agendadas, onde você pode configurar uma tarefa para implementar a configuração do agente teus Thin Client HP WES dispositivos alvo.

Tópicos relacionados

"Gerenciamento de dispositivos HP Thin Client a partir do console LANDesk" na página 984

Configurar os dispositivos HP ThinPro Linux

Antes de gerenciar seus dispositivos HP ThinPro Linux, você deve configurá-los com o agente LANDesk padrão (CBA ou Common Base Agent (Agente de Base Comum)). Isso os torna dispositivos gerenciados no banco de dados do núcleo LANDesk e permite que as diversas tarefas de gerenciamento sejam realizadas — incluindo as tarefas de Gerenciamento de hardwares e softwares de parceiros da LANDesk — por meio do console LANDesk.

LANDesk Management SuiteVersão9.5 suporta as HP ThinPro Linux plataformas seguintes:

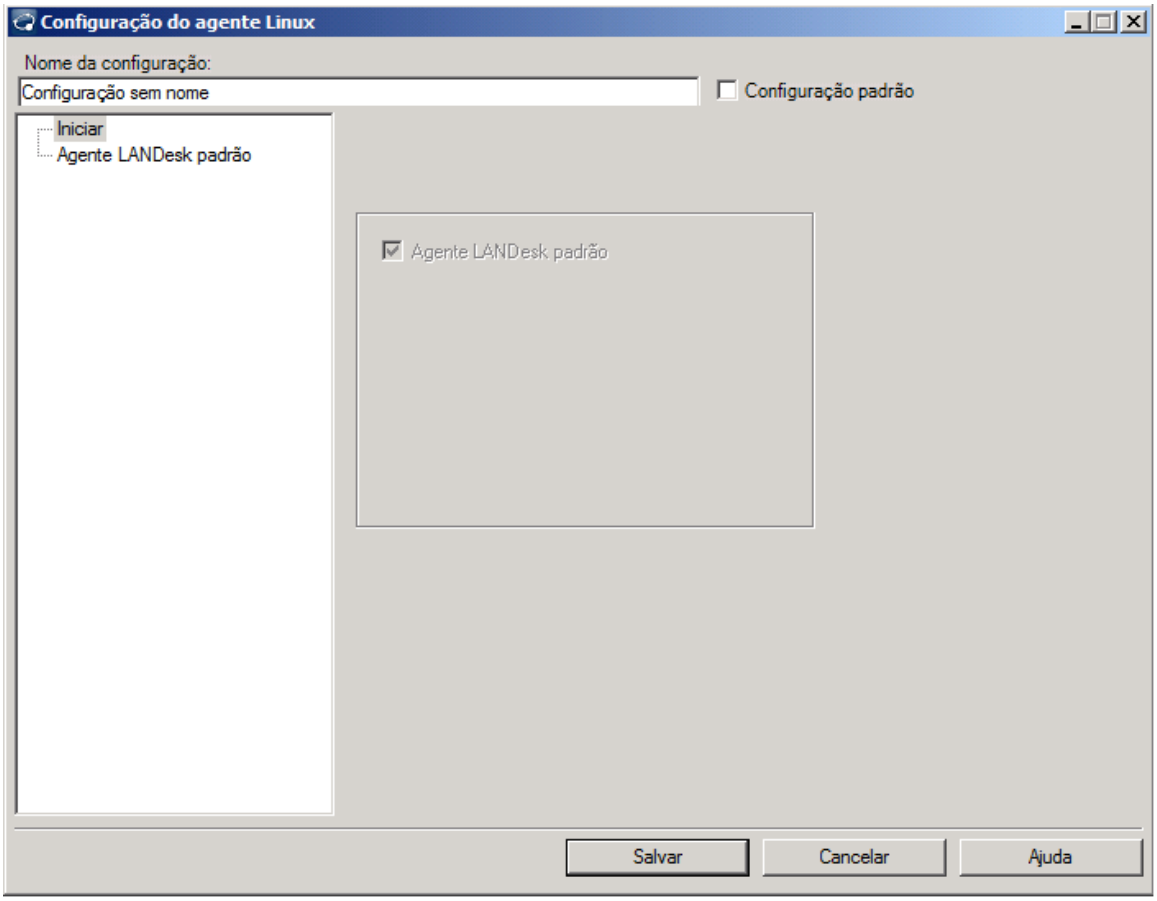
- HP ThinPro Linux Ubuntu

Distribuir o agente LANDesk em dispositivos HP ThinPro Linux

Para distribuir o agente LANDesk

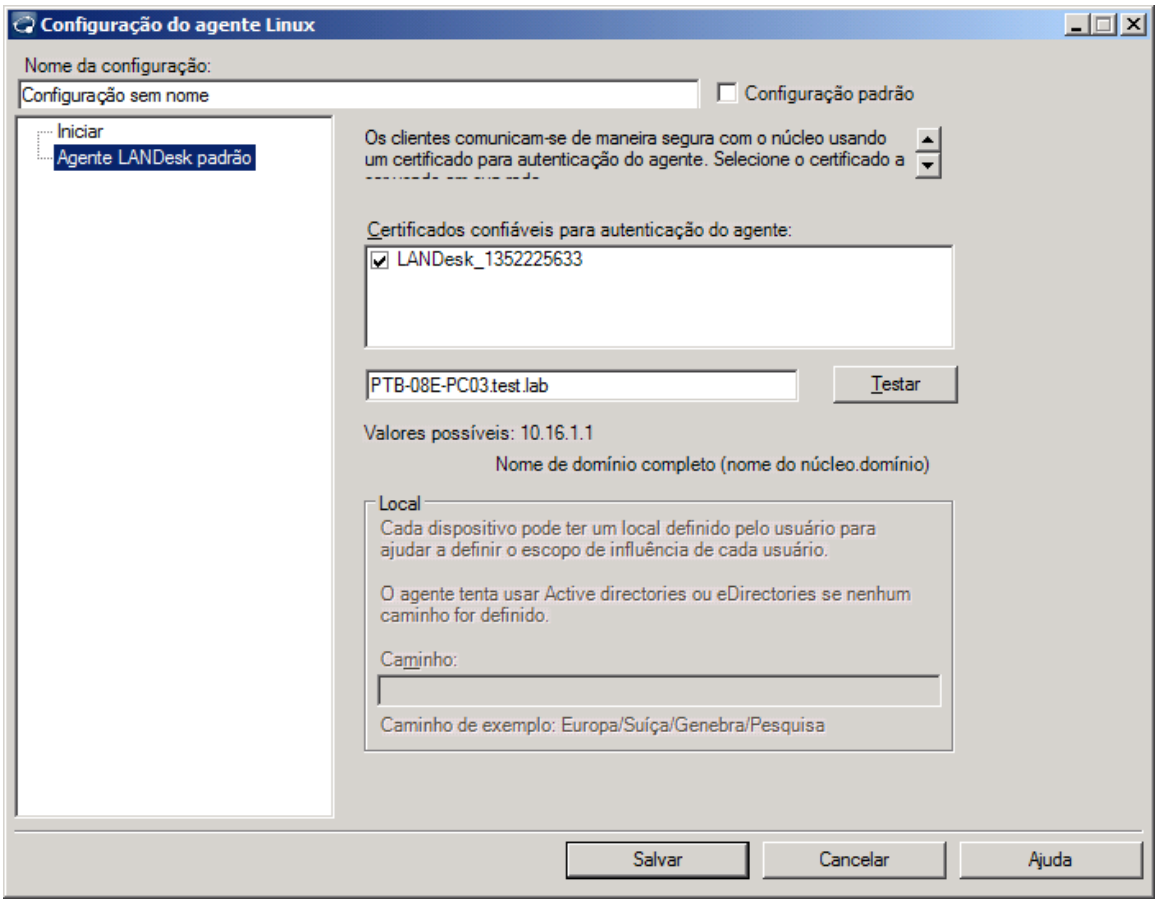
1. A partir do console, clique em **Ferramentas > Configuração > Configuração de agente** para abrir a caixa de diálogo Configuração de agente.
2. Clique com o botão direito em **Minha Configuração** e, em seguida, clique em **Configuração do novo agente HP ThinPro Linux**.

3. A caixa de diálogo Configuração de agente HP ThinPro Linux é uma versão reduzida da configuração de agente padrão do Windows. Inclui a página do agente LANDesk padrão.



4. Na página **Iniciar**, insira um nome único para a configuração.

5. Clique a **norma a LANDesk** página do agente e especifique as suas definições (clique em Ajuda para obter informações detalhadas).


Configuração do agente Linux
Nome da configuração:
Configuração sem nome
Configuração padrão
Iniciar
Agente LANDesk padrão
Os clientes comunicam-se de maneira segura com o núcleo usando um certificado para autenticação do agente. Selecione o certificado a
Certificados confiáveis para autenticação do agente:
LANDesk_1352225633
PTB-08E-PC03.test.lab
Testar
Valores possíveis: 10.16.1.1
Nome de domínio completo (nome do núcleo.domínio)
Local
Cada dispositivo pode ter um local definido pelo usuário para ajudar a definir o escopo de influência de cada usuário.
O agente tenta usar Active directories ou eDirectories se nenhum caminho for definido.
Caminho:
Caminho de exemplo: Europa/Suíça/Genebra/Pesquisa
Salvar
Cancelar
Ajuda

6. Clique em **Salvar**. Isso adiciona a tarefa para a ferramenta janela das Tarefas Agendadas, onde você pode configurar uma tarefa para implementar a configuração do agente teus HP ThinPro Linux dispositivos alvo.

Tópicos relacionados

"Gerenciamento de dispositivos HP Thin Client a partir do console LANDesk" na página 984

Acesse as ferramentas integradas HP no console LANDesk

Agora você pode fazer o logon no console LANDesk e acessar as ferramentas de Gerenciamento de hardwares HP que são adicionadas ao console LANDesk durante a instalação do software LANDesk Management Suite com Gerenciamento de hardwares HP.

No console, você também pode acessar componentes do inventário de dispositivos HP gerenciados, entre eles os periféricos de ponto-de-venda de varejo (RPOS).

O LANDesk plus HP Management acrescenta duas novas ferramentas da HP ao menu Configurar do console:

- **Configuração do BIOS da HP**
- **Configuração do TPM da HP**

Ela também acrescenta um novo HP-ferramenta específica para a janela da ferramenta de configurações de segurança do console:

- **Diretivas da HP Software**

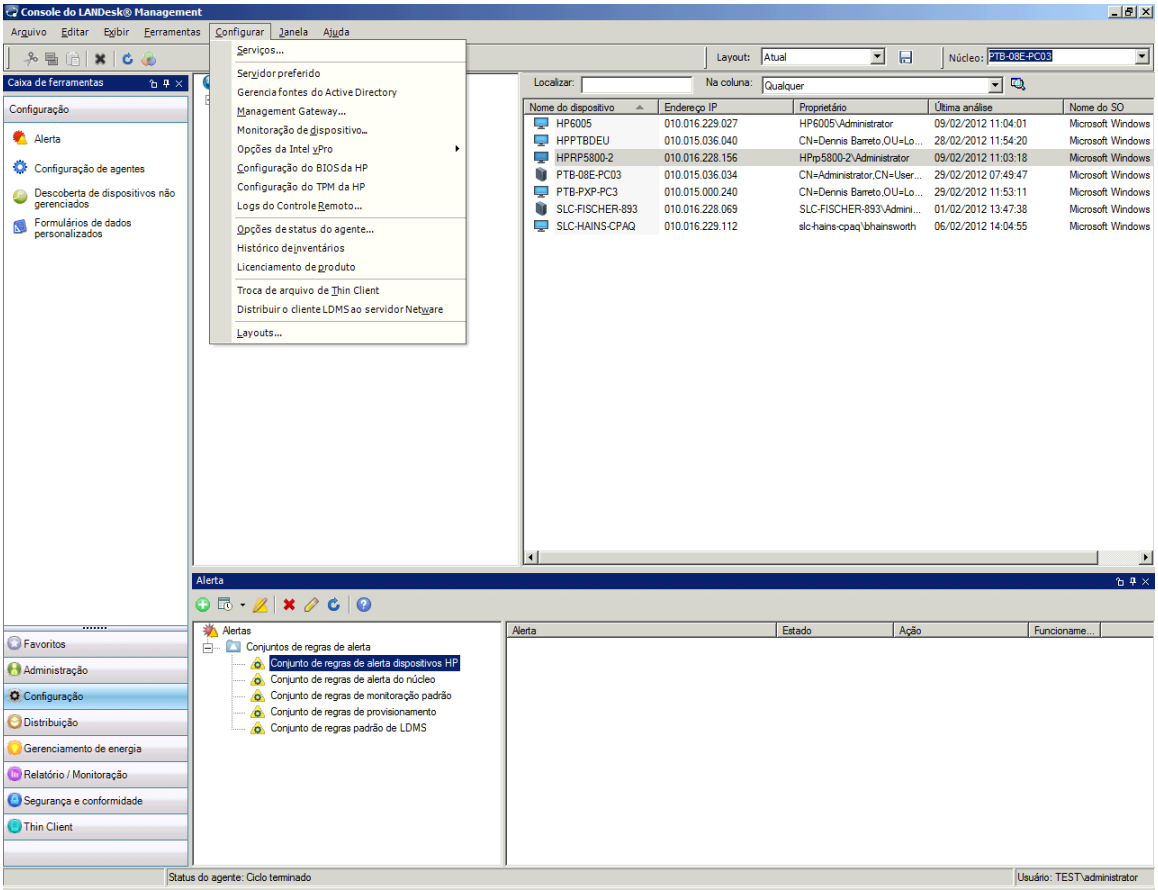
Para descrições dessas ferramentas integradas da HP, consulte "Ajuda para configuração de parâmetros do BIOS" na página 985, "Ajuda para a configuração do TPM" na página 986, e "Ajuda para configurações de diretivas de softwares da HP" na página 986 .

IMPORTANTE: Reinicie o console para ver as ferramentas
Você DEVE fechar e reiniciar o console LANDesk (assim como quaisquer outros consoles que você tenha no sistema LANDesk) para ver as novas ferramentas HP no menu **Configurar**.

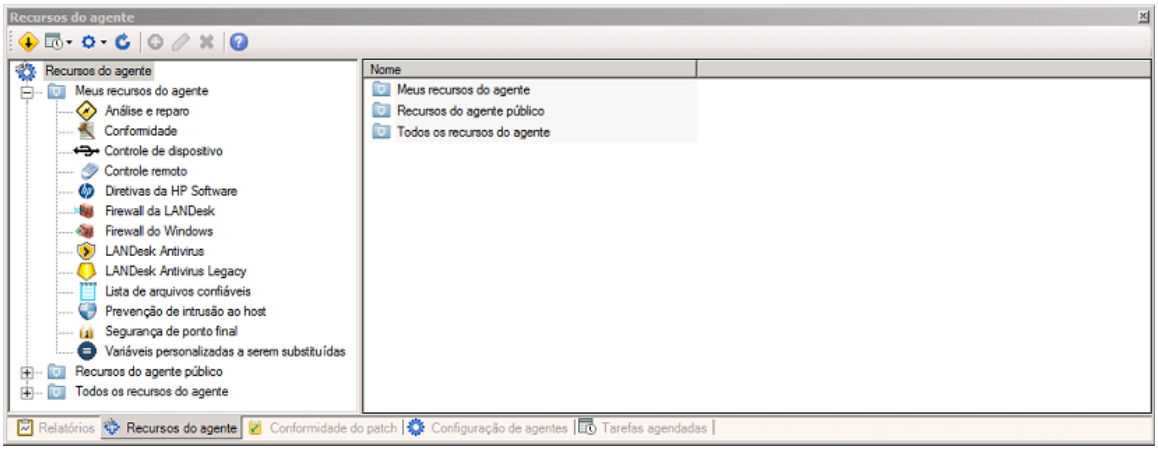
IMPORTANTE: Direitos de Administrador LANDesk necessário
Somente usuários com direitos de Administrador LANDesk conseguem ver e usar as ferramentas de Gerenciamento de hardwares HP.

Para acessar as ferramentas Gerenciamento de hardwares HP

1. No console, selecione um dispositivo gerenciado da HP na Tela de rede.
2. Clique no menu da ferramenta de Configuração e, em seguida, clique na ferramenta de **Configuração da HP** na lista que você deseja abrir.



3. OU. para a nova ferramenta de configurações de diretivas de softwares da HP, clique em **Ferramentas > Segurança e Conformidade > Configurações de Segurança**, abra o nó **Minhas configurações de segurança** e em **Diretivas de softwares da HP**.



Execute uma análise de inventário e veja o inventário de dispositivos HP

Após executar o analisador de inventário LANDesk em um dispositivo gerenciado da HP, você pode exibir os dados do Inventário no console da LANDesk.

Em vista do inventário de dispositivos, você vai encontrar o hardware e software seguintes dados do órgão:

- Dados de configuração do BIOS
- Dados do Assistente de energia da HP
- Verificação da bateria HP dados
- Gerenciador de Conexão da HP dados

Você também pode exibir o inventário para os dispositivos associados de Pontos-de-venda de varejo (RPOS) da HP.

NOTA: O
dispositivo de leitura de dados de inventário de dados de inventário de dispositivos é armazenado no banco de dados do núcleo da LANDesk. Pode ser visualizado e utilizado por várias ferramentas diferentes através do console da LANDesk: a visão de inventário, relatórios, consultas personalizadas, alertas, etc.

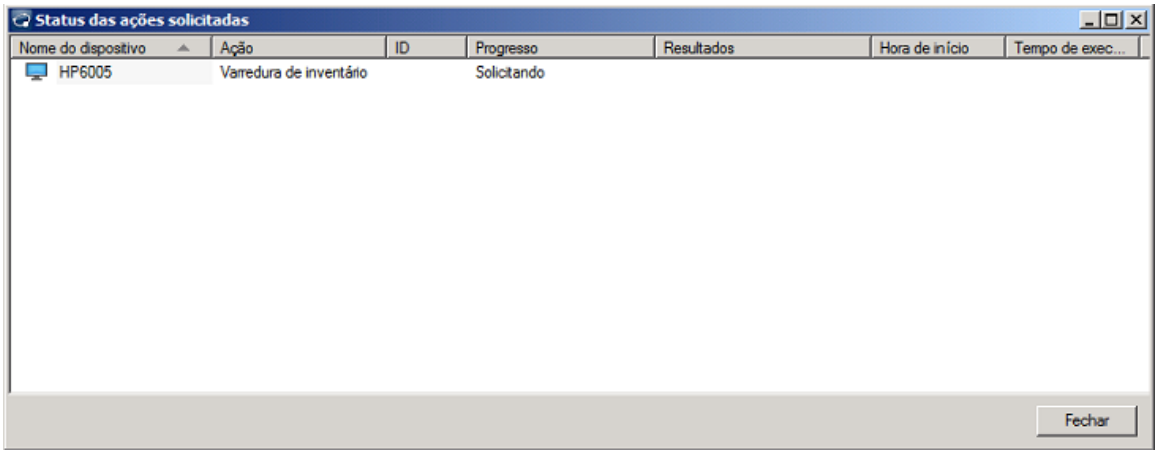
Execute uma análise de Inventário em um dispositivo gerenciado da HP

Este procedimento obtém informações de componentes de hardware e software de um dispositivo gerenciado e armazena-o no banco de dados núcleo da LANDesk.

Para executar uma análise de Inventário

1. No console, clique com o botão direito em um dispositivo gerenciado da HP para acessar seu menu de atalho.
2. Clique em **Análise de inventário** e selecione o tipo de análise que você quer executar.

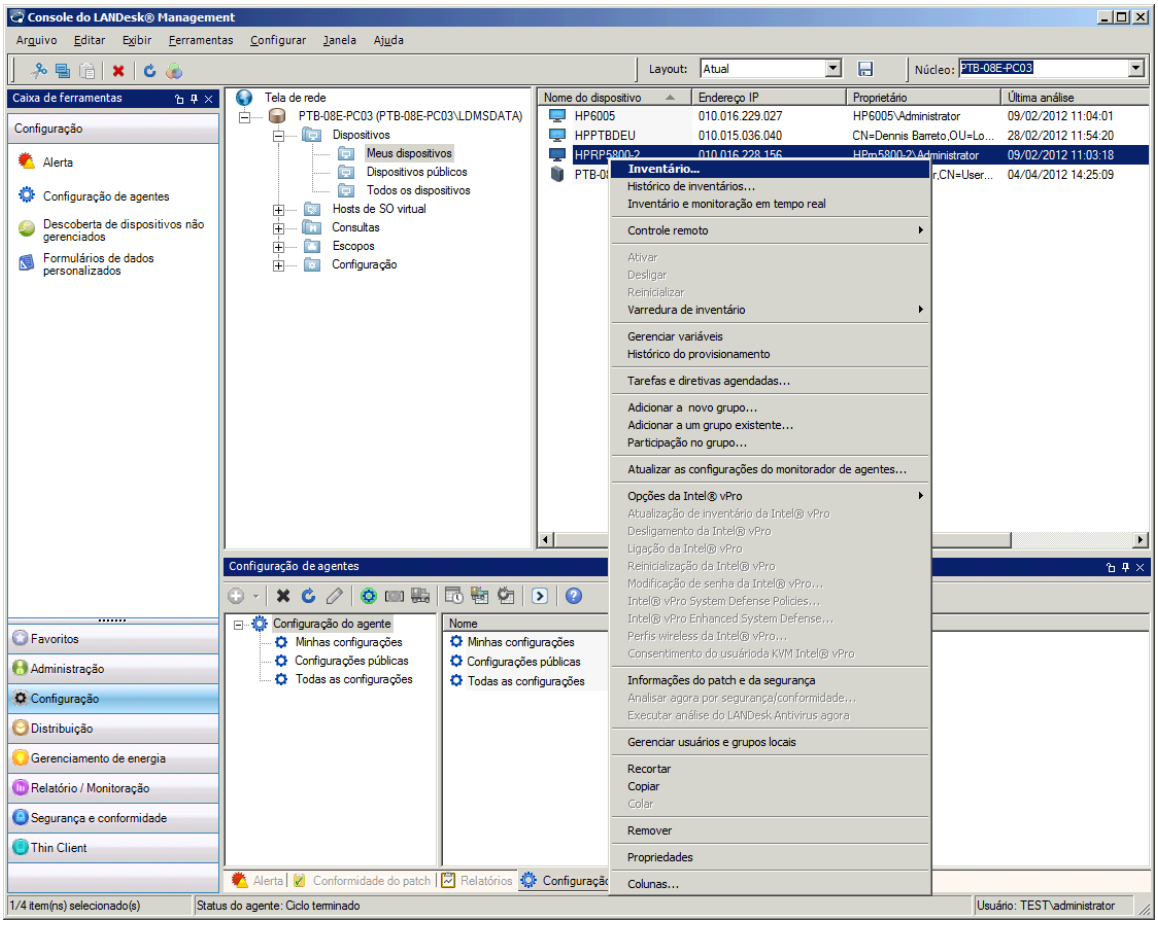
3. A janela de estado apresenta o progresso e outros detalhes para a ação solicitada.



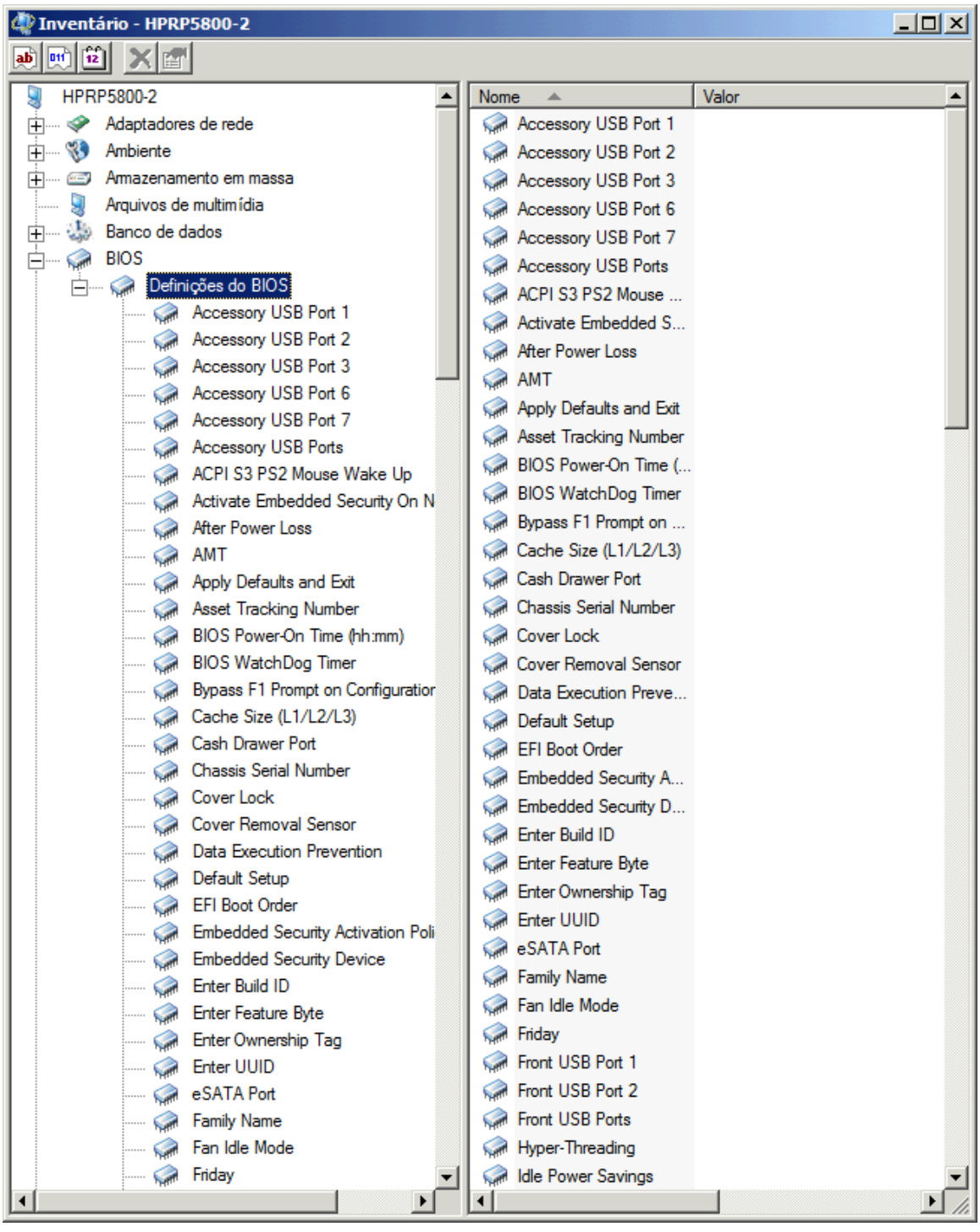
Exibir um inventário de dispositivo gerenciado da HP

Para exibir um inventário de dispositivo gerenciado da HP

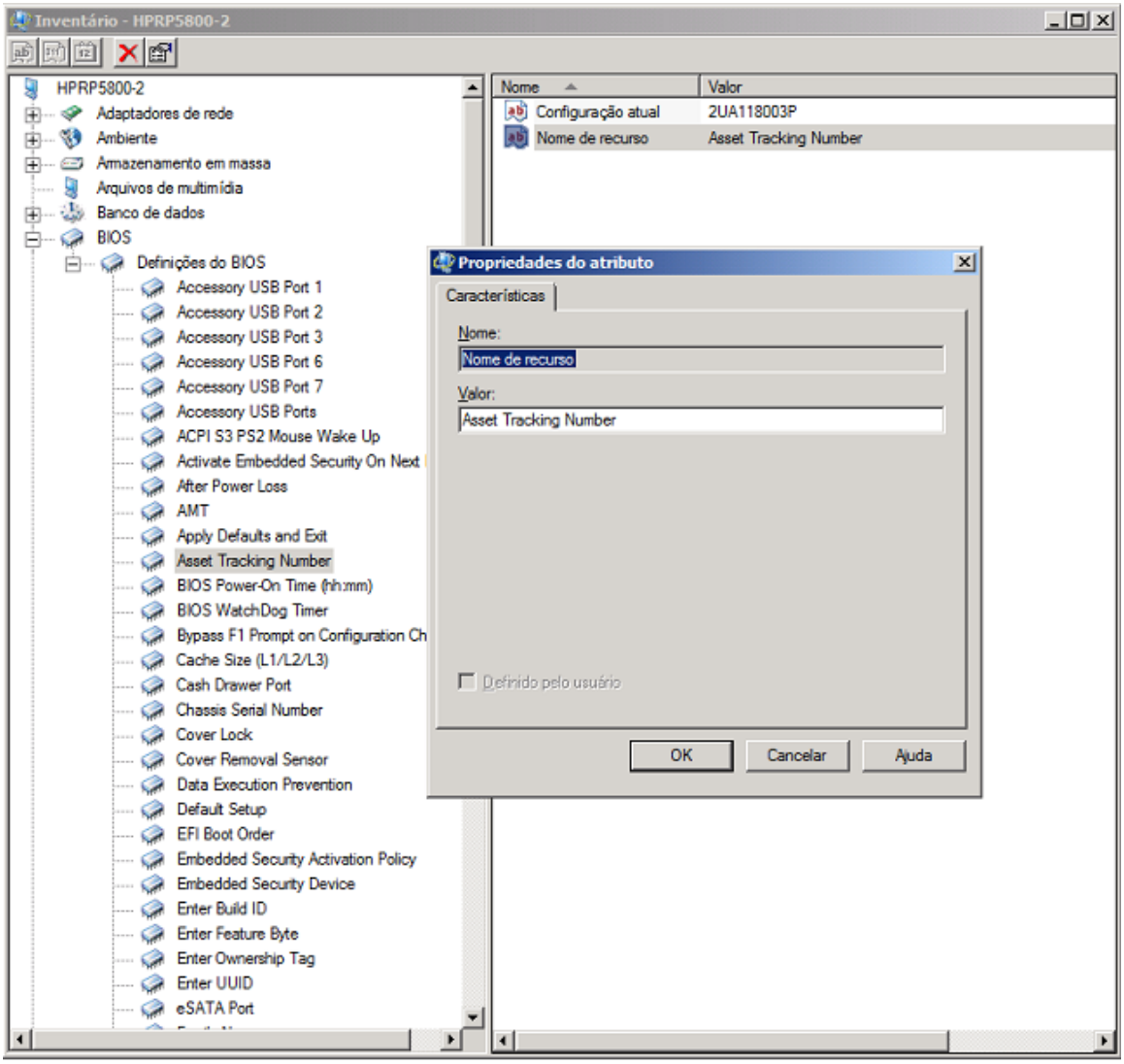
1. No console, clique com o botão direito em um dispositivo gerenciado da HP para acessar seu menu de atalho e clique em **Inventário**.



2. Na janela do inventário, você pode selecionar qual o tipo de dados digitalizados de HP para ver. Por exemplo, para ver o dispositivo da HP os dados das definições do BIOS, abra o componente **do BIOS** e, em seguida, abra o **BIOS Settings** nó.


Inventário - HPRP5800-2
HPRP5800-2
Adaptadores de rede
Ambiente
Armazenamento em massa
Arquivos de multimídia
Banco de dados
BIOS
Definições do BIOS
Accessory USB Port 1
Accessory USB Port 2
Accessory USB Port 3
Accessory USB Port 6
Accessory USB Port 7
Accessory USB Ports
ACPI S3 PS2 Mouse Wake Up
Activate Embedded Security On N
After Power Loss
AMT
Apply Defaults and Exit
Asset Tracking Number
BIOS Power-On Time (hh:mm)
BIOS WatchDog Timer
Bypass F1 Prompt on Configuratior
Cache Size (L1/L2/L3)
Cash Drawer Port
Chassis Serial Number
Cover Lock
Cover Removal Sensor
Data Execution Prevention
Default Setup
EFI Boot Order
Embedded Security Activation Poli
Embedded Security Device
Enter Build ID
Enter Feature Byte
Enter Ownership Tag
Enter UUID
eSATA Port
Family Name
Fan Idle Mode
Friday
Nome
Valor
Accessory USB Port 1
Accessory USB Port 2
Accessory USB Port 3
Accessory USB Port 6
Accessory USB Port 7
Accessory USB Ports
ACPI S3 PS2 Mouse ...
Activate Embedded S...
After Power Loss
AMT
Apply Defaults and Exit
Asset Tracking Number
BIOS Power-On Time (...
BIOS WatchDog Timer
Bypass F1 Prompt on ...
Cache Size (L1/L2/L3)
Cash Drawer Port
Chassis Serial Number
Cover Lock
Cover Removal Sensor
Data Execution Preve...
Default Setup
EFI Boot Order
Embedded Security A...
Embedded Security D...
Enter Build ID
Enter Feature Byte
Enter Ownership Tag
Enter UUID
eSATA Port
Family Name
Fan Idle Mode
Friday
Front USB Port 1
Front USB Port 2
Front USB Ports
Hyper-Threading
Idle Power Savings

3. Para ver as propriedades de um atributo específico, selecione o atributo desejado na lista e, em seguida, faça duplo clique sobre uma propriedade para a armação da direita.

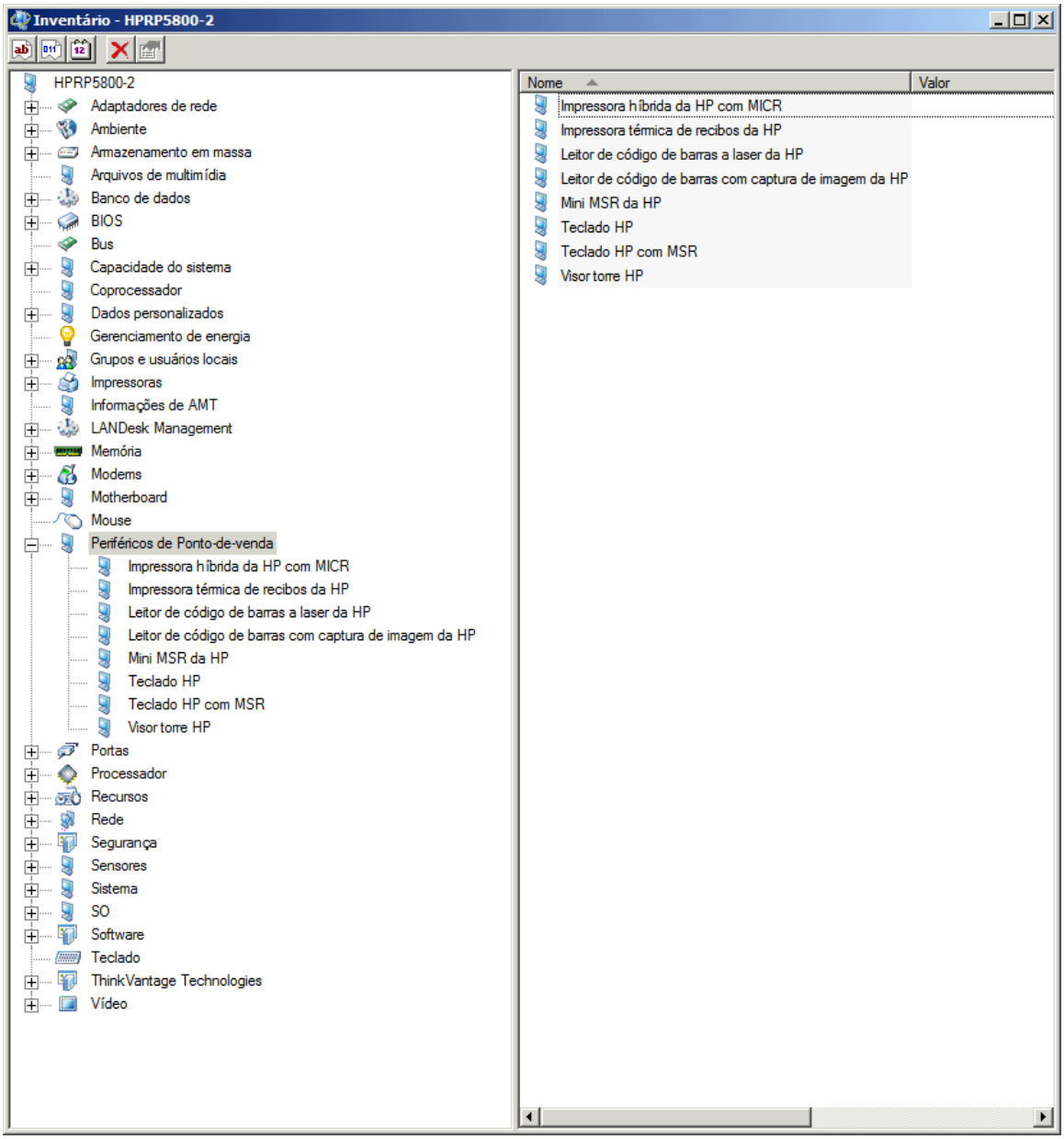


4. Clique em **OK** para fechar a caixa de diálogo propriedades.
5. Você também pode abrir o nó da **Hewlett-Packard** para exibir os dados específicos da HP, tais como: Dados do Assistente de energia da HP, do Verificador de bateria da HP e do Gerenciador de conexões da HP. Para obter mais informações, consulte "Use o Assistente de energia da HP" na página 967, "Use o Verificador de bateria da HP" na página 969 e "Use o Gerenciador de conexões da HP" na página 970.

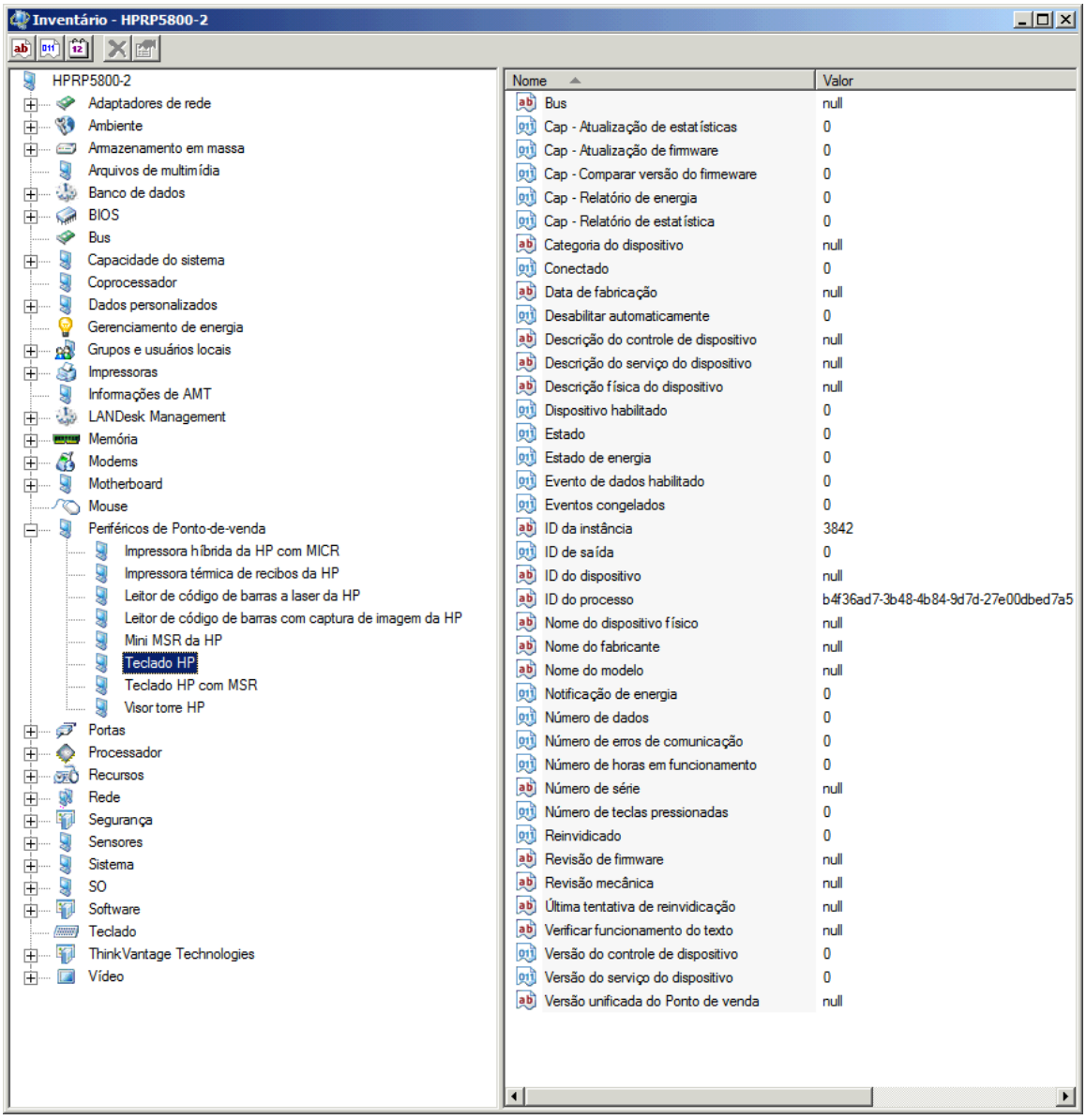
Exibir um inventário de um dispositivo periférico da HP para Pontos-de-venda de varejo (RPOS)

Para exibir o inventário de um dispositivo periférico da HP para Pontos-de-venda de varejo (RPOS)

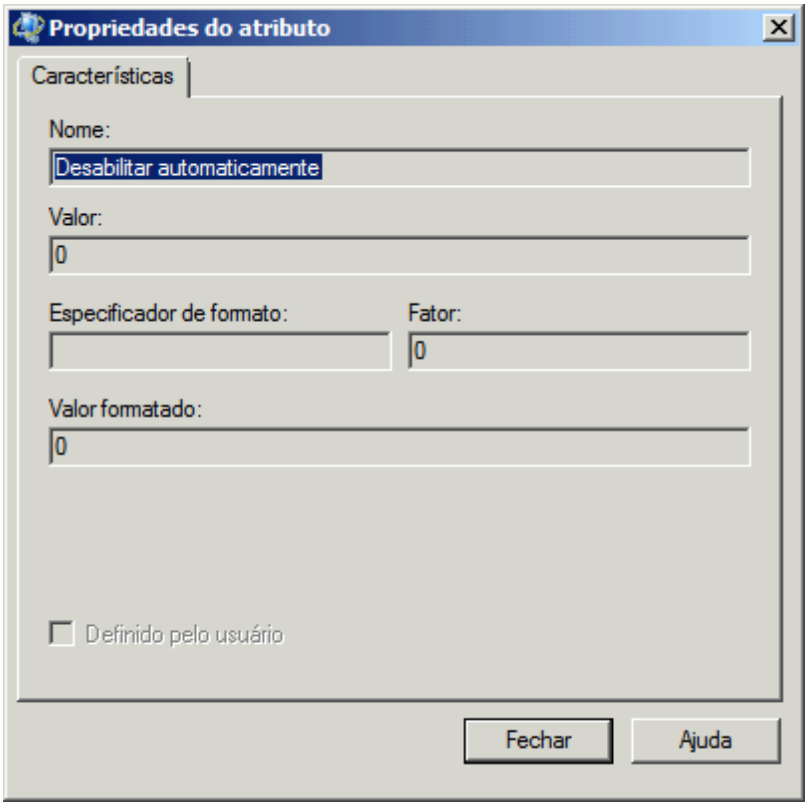
1. No console, clique com o botão direito em um dispositivo gerenciado da HP e em **Inventário > Periféricos para ponto-de-venda de varejo**.



2. Para ver os atributos e valores do inventário de um dispositivo RPOS específico, selecione o dispositivo (por exemplo, **Teclado HP**).



3. Para exibir as propriedades de um atributo específico, clique duas vezes no nome do atributo (por exemplo, **Desabilitar automaticamente**).



IMPORTANTE: Como a LANDesk Management Suite obtém e armazena dados de dispositivo da HP
O servidor do núcleo da LANDesk executa um utilitário proprietário (o executável do LDHPMgr) que reúne dados específicos dos dispositivos gerenciados da HP em rede. Outro utilitário (o executável do HPScanner) coloca a informação no banco de dados do núcleo da LANDesk.

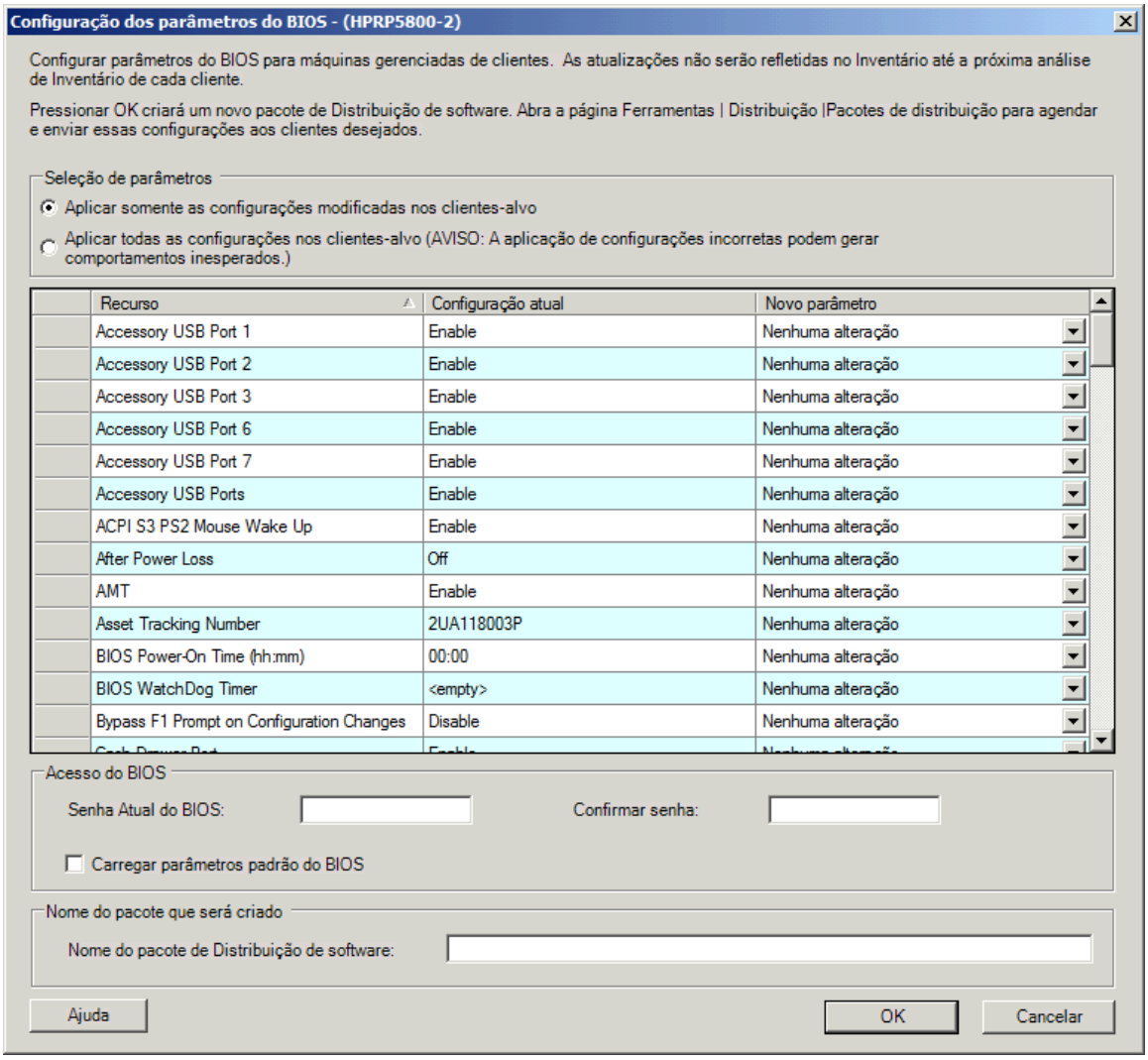
Crie e distribua configurações de BIOS da HP para dispositivos HP

Para alterar remotamente as configurações do BIOS em um ou mais dispositivos gerenciados da HP, configure o BIOS no console da LANDesk e distribua as configurações para os dispositivos alvo da HP.

IMPORTANTE: Nova análise de inventário necessária para que as alterações de configurações do BIOS apareçam no Inventário
Qualquer alteração que você fizer na configuração do BIOS de um dispositivo gerenciado da HP usando a distribuição de um pacote de configuração de parâmetros do BIOS não será aplicado no inventário do dispositivo até *após* a próxima análise do inventário.

Para criar um pacote de configuração de parâmetros do BIOS da HP

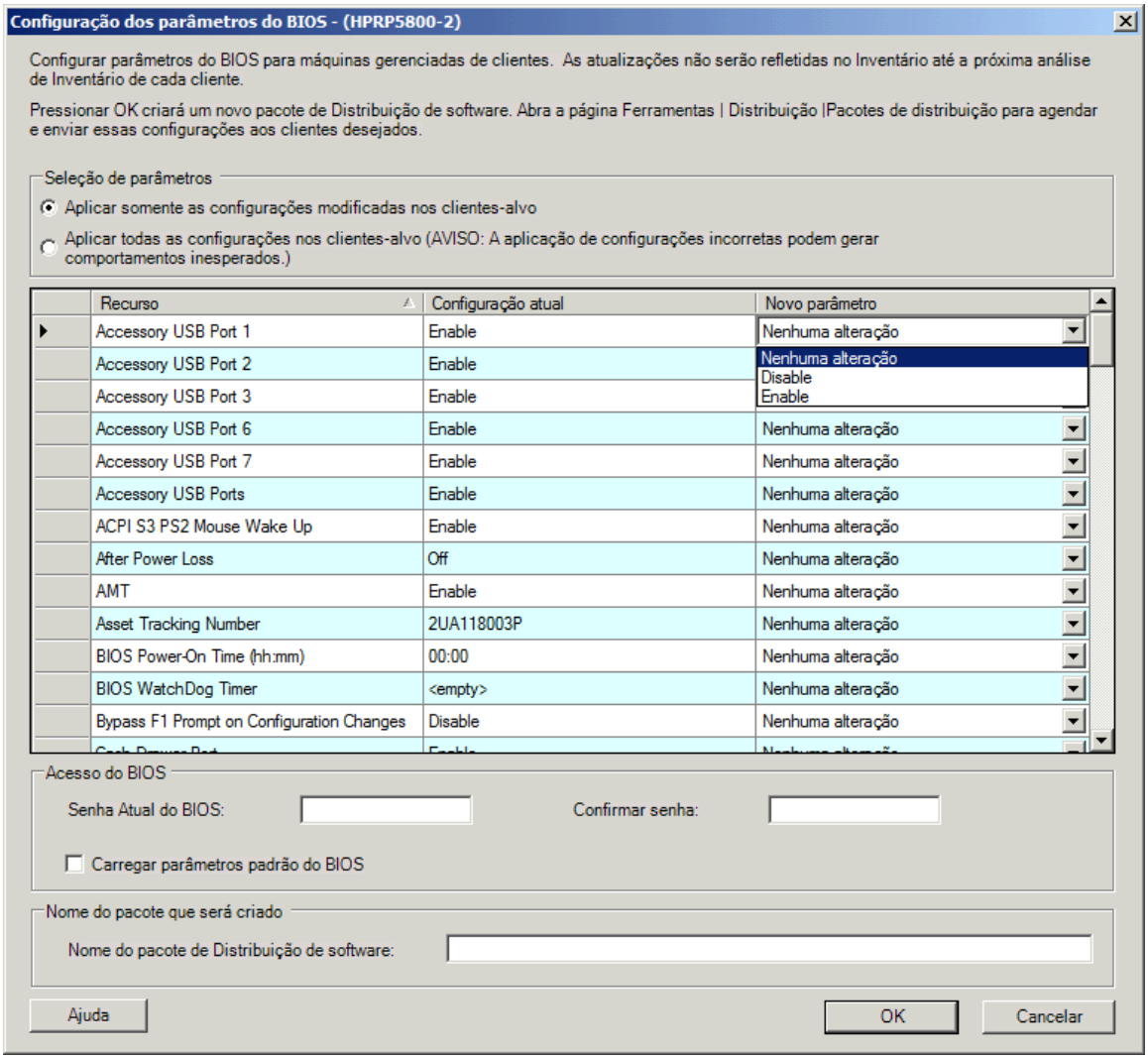
1. No console, selecione um dispositivo gerenciado da HP a partir da Tela de rede.
2. Clique em **Ferramentas > Configurar > Configuração do BIOS da HP**.


Configuração dos parâmetros do BIOS - (HPRP5800-2)
Configurar parâmetros do BIOS para máquinas gerenciadas de clientes. As atualizações não serão refletidas no Inventário até a próxima análise de Inventário de cada cliente.
Pressionar OK criará um novo pacote de Distribuição de software. Abra a página Ferramentas | Distribuição |Pacotes de distribuição para agendar e enviar essas configurações aos clientes desejados.
Seleção de parâmetros
Aplicar somente as configurações modificadas nos clientes-alvo
Aplicar todas as configurações nos clientes-alvo (AVISO: A aplicação de configurações incorretas podem gerar comportamentos inesperados.)
Recurso
Configuração atual
Novo parâmetro
Accessory USB Port 1 Enable Nenhuma alteração
Accessory USB Port 2 Enable Nenhuma alteração
Accessory USB Port 3 Enable Nenhuma alteração
Accessory USB Port 6 Enable Nenhuma alteração
Accessory USB Port 7 Enable Nenhuma alteração
Accessory USB Ports Enable Nenhuma alteração
ACPI S3 PS2 Mouse Wake Up Enable Nenhuma alteração
After Power Loss Off Nenhuma alteração
AMT Enable Nenhuma alteração
Asset Tracking Number 2UA118003P Nenhuma alteração
BIOS Power-On Time (hh:mm) 00:00 Nenhuma alteração
BIOS WatchDog Timer <empty> Nenhuma alteração
Bypass F1 Prompt on Configuration Changes Disable Nenhuma alteração
Acesso do BIOS
Senha Atual do BIOS:
Confirmar senha:
Carregar parâmetros padrão do BIOS
Nome do pacote que será criado
Nome do pacote de Distribuição de software:
Ajuda
OK
Cancelar

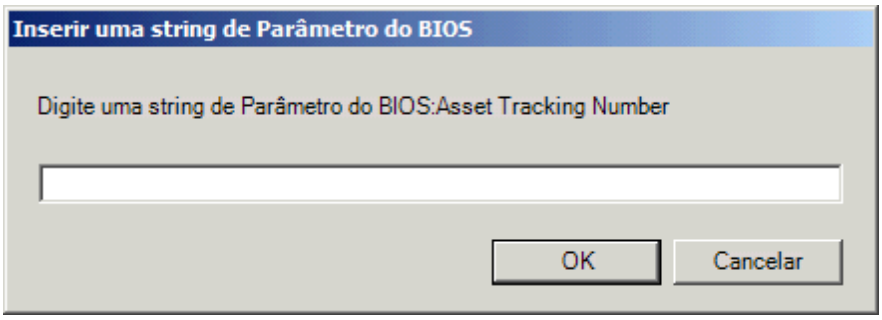
3. Digite um nome exclusivo para o pacote de configuração do BIOS da HP (na parte inferior da caixa de diálogo).
4. Selecione entre aplicar *somente* as configurações modificadas do BIOS em dispositivos alvo da HP ou em aplicar TODAS as configurações do BIOS aos dispositivos alvo.

   AVISO: Configurações mal aplicadas podem causar comportamentos não-intencionais.

5. Para alterar o parâmetro de um recurso do BIOS específico, selecione o recurso na lista e clique na **seta para baixo** na coluna Novo parâmetro. Dependendo do tipo de recurso do BIOS, um menu suspenso é exibido e você pode selecionar o parâmetro desejado, como exibido neste exemplo:



Ou, se o recurso exige um valor de string de texto válido, uma caixa de texto é exibida para que você insira o valor, conforme exibido neste exemplo:



6. Faça todas as mudanças ou atualizações dos parâmetros do BIOS que desejar.
7. Para acessar o BIOS dos dispositivos da HP. você tem que inserir e confirmar a **Senha de BIOS** atual.
8. Clique em **OK**.

Tópicos relacionados

Agora você pode distribuir a configuração usando a ferramenta Tarefas agendadas. Para obter informações detalhadas sobre como usar a ferramenta Tarefas agendadas, veja:

"Agendamento de tarefas" na página 227

"Usar a janela Tarefas agendadas" na página 228

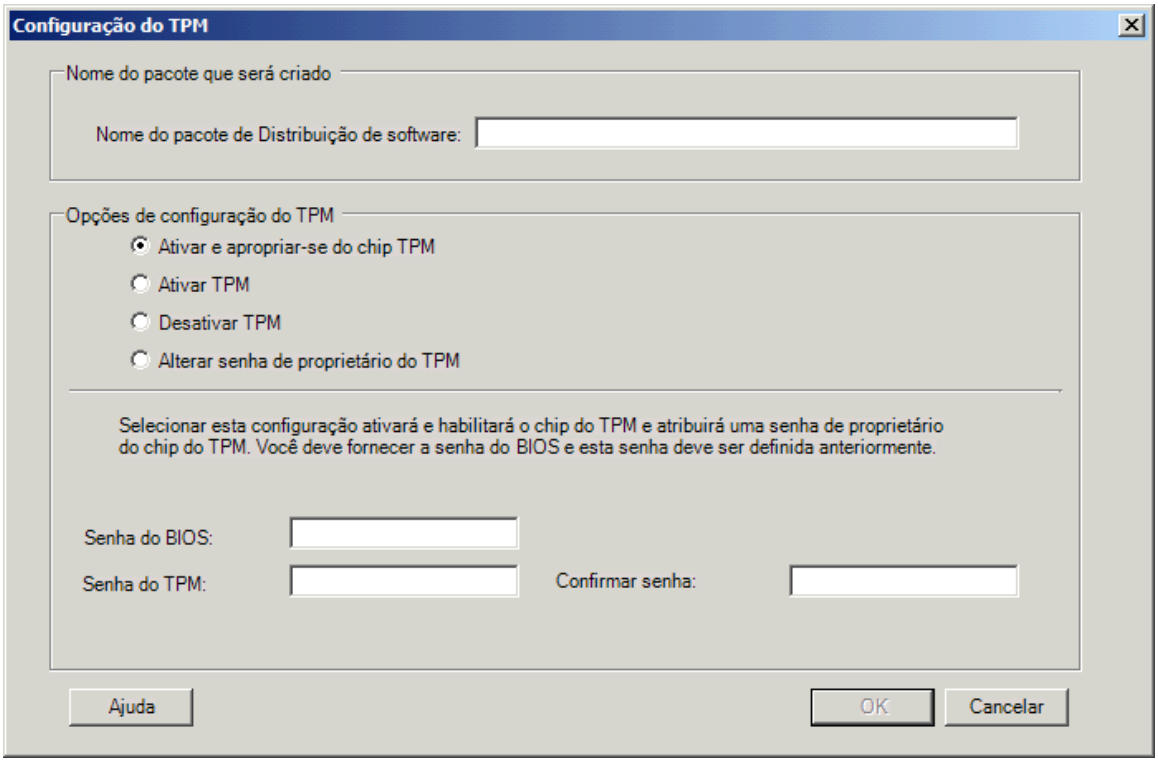
Crie e distribua configurações de chip TPM da HP para dispositivos HP

Você pode usar esta ferramenta para remotamente alterar as Platform Module (TPM) chip definições confiáveis de segurança sobre um ou mais de seus dispositivos gerenciados HP. Para fazer isso, configure as definições de TPM no console da LANDesk e distribua as configurações para os dispositivos-alvo da HP.

IMPORTANTE: O Windows XP não é suportado
o HP chip TPM ferramenta de regulação não é suportada em dispositivos HP executando o sistema operacional Windows XP.

Para criar um pacote de configurações do TPM da HP

1. No console, selecione um ou mais dispositivos gerenciados da HP a partir da Tela de rede.
2. Clique em **Ferramentas > Configurar > Configuração do TPM da HP**.


Configuração do TPM
Nome do pacote que será criado
Nome do pacote de Distribuição de software:
Opções de configuração do TPM
Ativar e apropriar-se do chip TPM
Ativar TPM
Desativar TPM
Alterar senha de proprietário do TPM
Selecionar esta configuração ativará e habilitará o chip do TPM e atribuirá uma senha de proprietário do chip do TPM. Você deve fornecer a senha do BIOS e esta senha deve ser definida anteriormente.
Senha do BIOS:
Senha do TPM:
Confirmar senha:
Ajuda
OK
Cancelar

3. Digite um nome exclusivo para o pacote de parâmetros de Configuração do TPM da HP.
4. Selecione **Habilitar** ou **Desabilitar** o chip TPM do dispositivo HP; ou **Habilitar e apropriar-se** ou **Alterar a senha de proprietário do TPM**. Dependendo de quais opções você selecionar, os controles na parte inferior da caixa de diálogo mudarão para refletir a ação escolhida.
5. Para apropriar-se do chip TPM, você precisará inserir a senha do BIOS previamente definida. Caso contrário, será necessário inserir a senha do TPM para as outras opções.
6. Clique em **OK**.

Tópicos relacionados

Agora você pode distribuir a configuração usando a ferramenta Tarefas agendadas. Para obter informações detalhadas sobre como usar a ferramenta Tarefas agendadas, veja:

"Agendamento de tarefas" na página 227

"Usar a janela Tarefas agendadas" na página 228

Use o Assistente de energia da HP

Assistente de energia da HP e Verificação de bateria HP ajudam a controlar e optimizar o consumo de energia dos dispositivos HP, e aumentar a sua performance.

Assistente de energia da HP permite que você configure atividade do poder e diretivas de utilização dos dispositivos gerenciados HP. Você pode controlar o consumo de energia em toda a sua rede, aplicar diretivas padrão para todos os seus dispositivos de HP, poupar dinheiro e aumentar a produtividade do utilizador final.

IMPORTANTE: Verifique se a versão correta da Assistente de energia da HP
o Assistente de energia da HP software instalar deve ser versão 2.1 ou superior.

Assistente de energia da HP opções são utilizados para criar uma HP Software diretiva. Em outras palavras, você pode usar a ferramenta Diretivas de softwares da HP para configurar o Assistente de energia, atribuir a diretiva a uma tarefa de Mudança de configuração e, em seguida, usar a ferramenta Tarefas agendadas para distribuir a diretiva (composta de eventos do Assistente de energia da HP) a dispositivos alvo da HP.

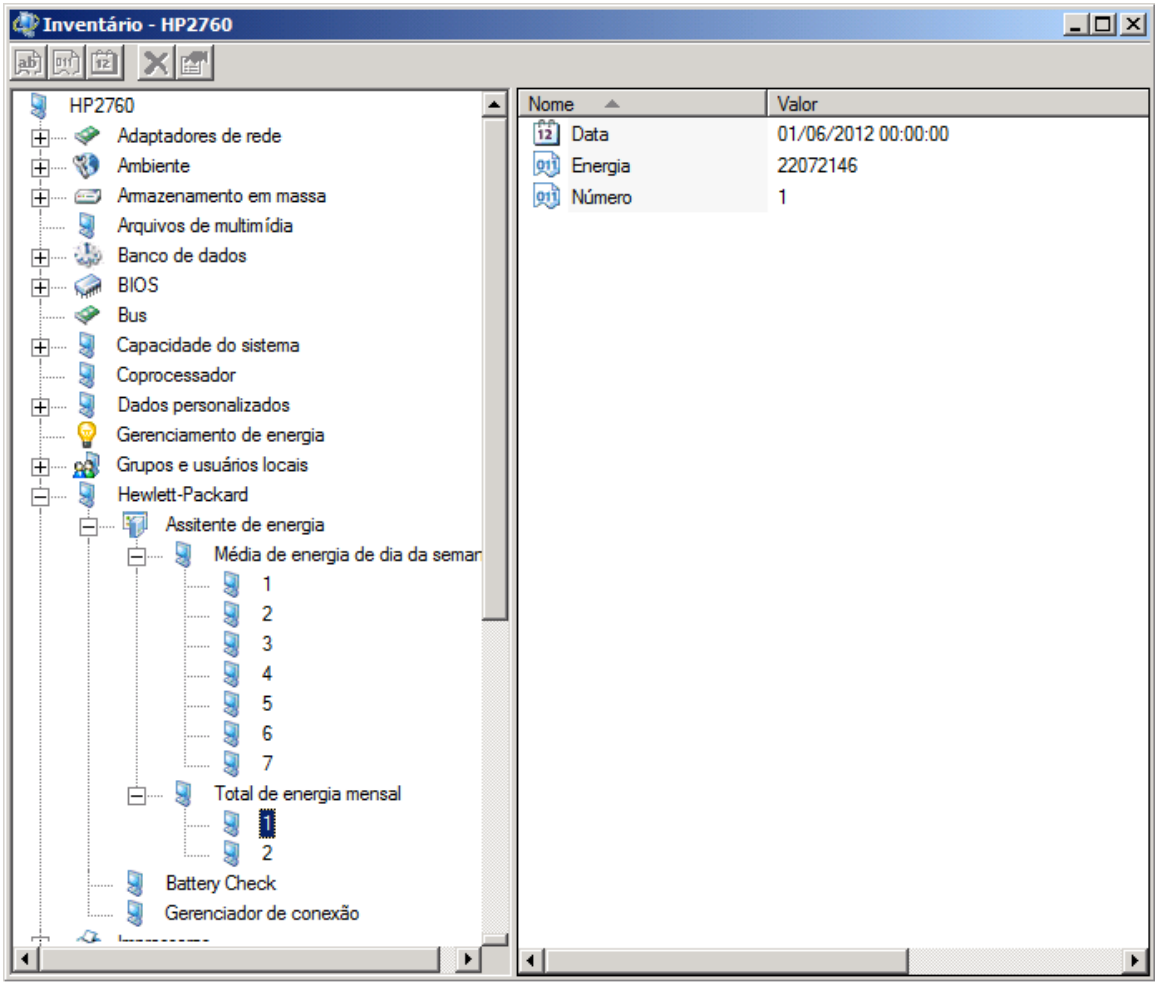
Para obter instruções passo-a-passo para este procedimento, consulte "Criar e distribuir configurações de diretivas de softwares da HP para dispositivos HP" na página 971 .

Após distribuir uma diretiva de Assistente de energia da HP nos dispositivos, e eles já foram analisados, os dados de uso de energia podem ser visualizados no inventário do dispositivo. (**NOTA:** Estes dados podem também ser visualizados no novo HP-relatórios específicos da ferramenta de relatórios.)

Para visualizar os dados do Assistente de energia da HP no inventário

1. Selecione um dispositivo da HP da **Tela de rede** no console.
2. Clique com o botão direito em configurações e clique em **Inventário**.

3. Abra o nó **da Hewlett-Packard** , abrir o nó do **Assistente de energia** e selecione qualquer um dos componentes para ver os valores dos atributos.



Use o Verificador de bateria da HP

Verificação da bateria HP fornece informações úteis sobre o estado da bateria e estado do dispositivo da HP. Você pode usar esta informação para obter o máximo dos seus investimentos em hardware e a planear e preparar-se para substituir baterias velhas ou defeituosas.

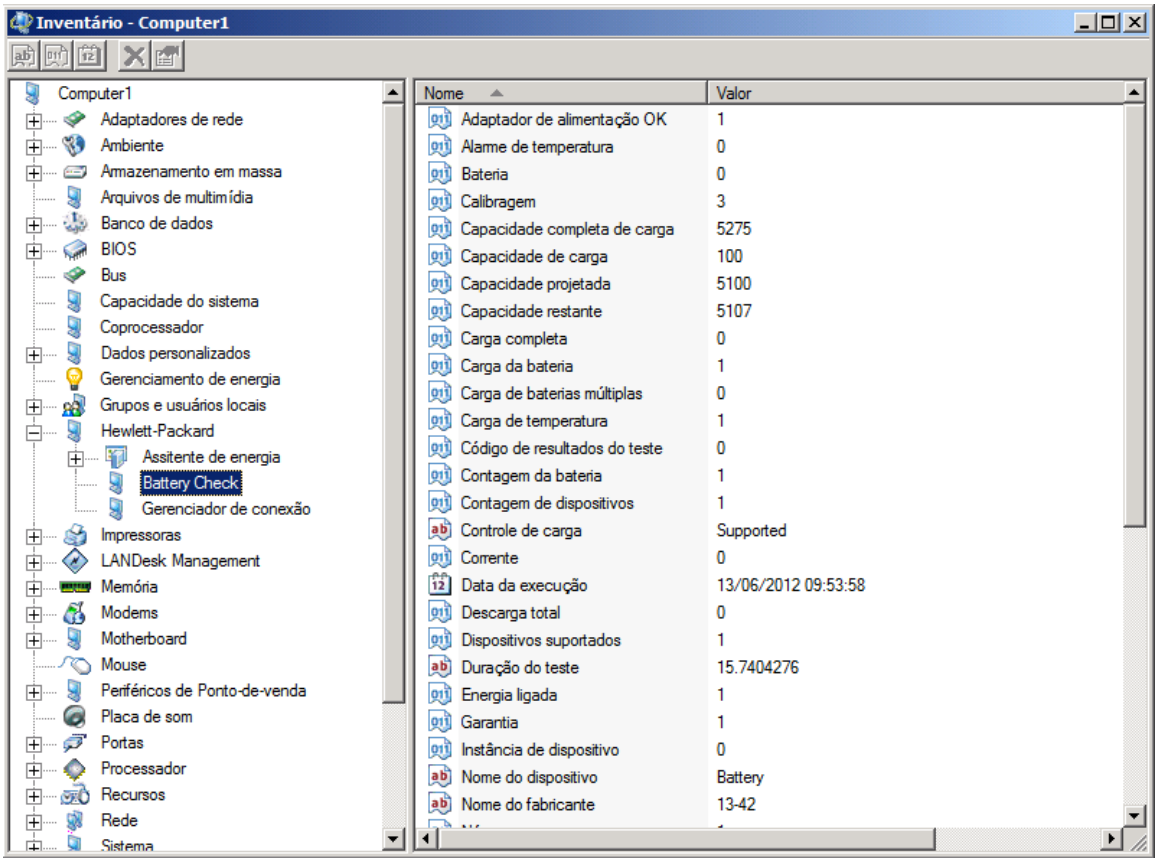
IMPORTANTE: Verifique se a versão correta da verificação da bateria HP
A HP software de verificação de bateria que você instalar deve ser versão 4.1 ou superior.

IMPORTANTE: Verificação da bateria HP não pode ser instalado em um dispositivo que já foi Assistente de Suporte da HP
a fim de instalar a HP software de verificação de bateria, você deve primeiro certificar-se de que a Assistente de Suporte HP Utility não está instalado no dispositivo da HP. Se for, você deve desinstalar Assistente de Suporte HP e depois instalar HP Bateria verificar (versão 4.1 ou superior).

Ao contrário do Assistente de energia da HP, HP Bateria verificar por si não é configurável. O analisador funciona a cada 14 dias e as informações analisadas são inseridas no banco de dados da LANDesk, você poderá consultá-las no inventário de dispositivos. (**NOTA:** Estes dados podem também ser visualizados no novo HP-relatórios específicos da ferramenta de relatórios.)

Para ver a HP Bateria Verificar dados do inventário

1. Selecione um dispositivo da HP da **Tela de rede** no console.
2. Clique com o botão direito em configurações e clique em **Inventário**.
3. Abra o nó **da Hewlett-Packard** , e selecione **bateria** para ver todos os dados.



Use o Gerenciador de conexões da HP

Gerenciador de Conexão da HP proporciona informação útil sobre as placas de rede do dispositivo da HP. Esta informação é muito útil para ativar a placa de rede (por exemplo, você pode encontrar o número do IMEI do cartão em um inventário de um dispositivo lido HP sem ter de abrir a máquina), e no Monitoramento e Gerenciamento conectividade de rede e atividade.

IMPORTANTE: Verifique se a versão correta do gerenciador de conexão da HP
A HP Ligação software Manager você instalar deve ser versão 4.1 ou superior.

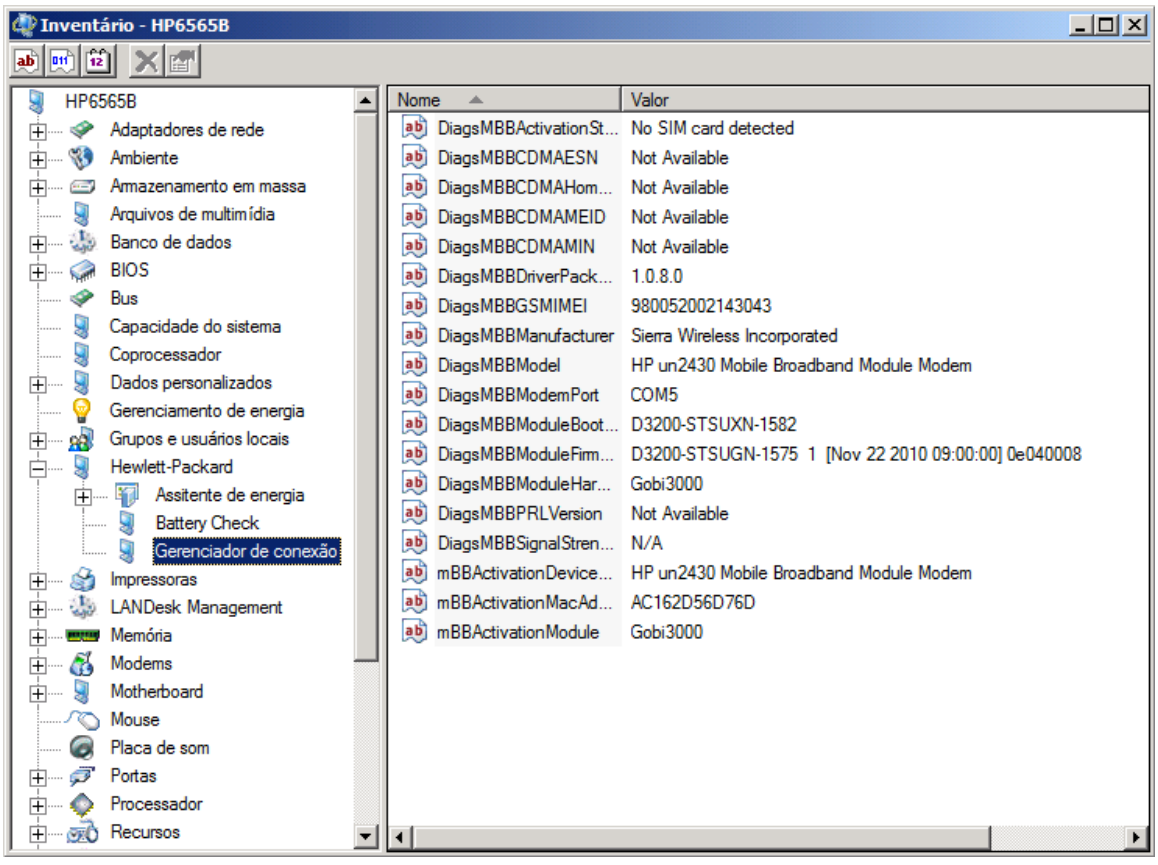
IMPORTANTE: A

conexão da HP com cartões de rede suportado Manager suporta compatível com HP apenas cartões de rede.

Ao contrário do Assistente de energia da HP, Gerenciador de Conexão da HP não é configurável. O analisador funciona uma vez ao dia e as informações analisadas são inseridas no banco de dados da LANDesk, você poderá consultá-las no inventário de dispositivos. (**NOTA:** Estes dados podem também ser visualizados no novo HP-relatórios específicos da ferramenta de relatórios.)

Para visualizar o gerenciador de conexão da HP dados do inventário

1. Selecione um dispositivo da HP da **Tela de rede** no console.
2. Clique com o botão direito em configurações e clique em **Inventário**.
3. Abra o nó **da Hewlett-Packard** , e selecione **Gestor de Ligação** ver todos os dados.



Criar e distribuir configurações de diretivas de softwares da HP para dispositivos HP

Use o diretivas de softwares da HP para configurar e implementar configurações do Assistente de energia da HP aos dispositivos gerenciados da HP. Estas configurações permitem que você otimize o uso da energia e desempenho com as ações padrão de energia da HP e perfis que podem ser agendados em horas e duração específicos.

As ações padrão de energia da HP são:

- Hibernar
- Repouso
- Nos dias

Os perfis padrão de gerenciamento de energia da HP são:

- Economia de energia
- Equilibrado
- Optimizado
- Alto desempenho

Primeiro, configure as definições de energia com a ferramenta Diretivas de softwares da HP, atribua essa diretiva a uma tarefa de mudanças de configurações e agente a tarefa para execução nos dispositivos HP desejados.

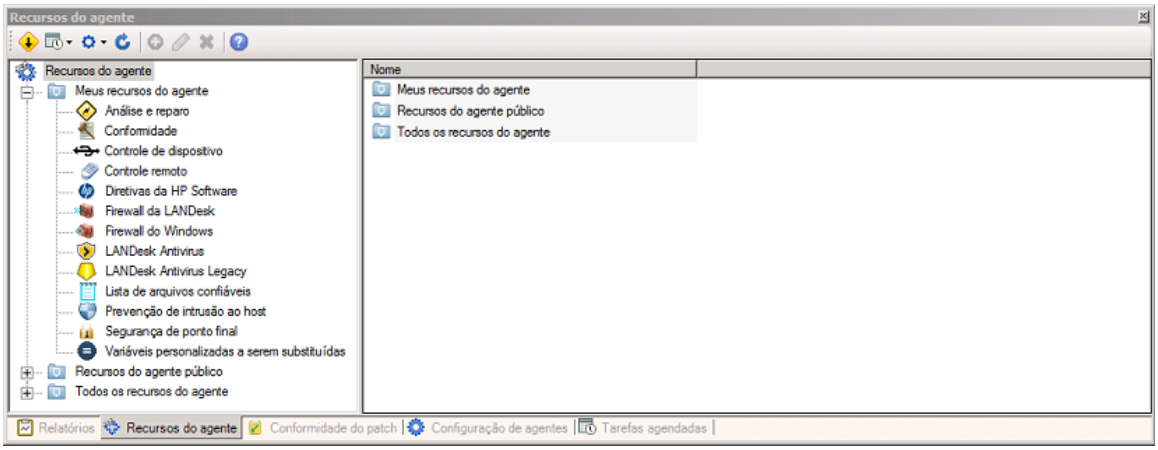
NOTA: Verificador de bateria da HP e Gerenciador de conexões da HP são executados pelo servidor núcleo
As ferramentas Verificador de bateria da HP e Gerenciador de conexões da HP não são tarefas agendadas no consoles da LANDesk. O servidor do núcleo da LANDesk é executado automaticamente esses scans da HP e adiciona os dados no banco de dados do núcleo. Verificação da bateria HP leituras dispositivos HP cada 14 dias. Gerenciador de Conexão da HP leituras dispositivos HP uma vez por dia.

Diretivas de softwares de HP fazem parte da ferramenta de configurações de segurança (**> Segurança e conformidade > Configurações de Segurança Ferramentas**).

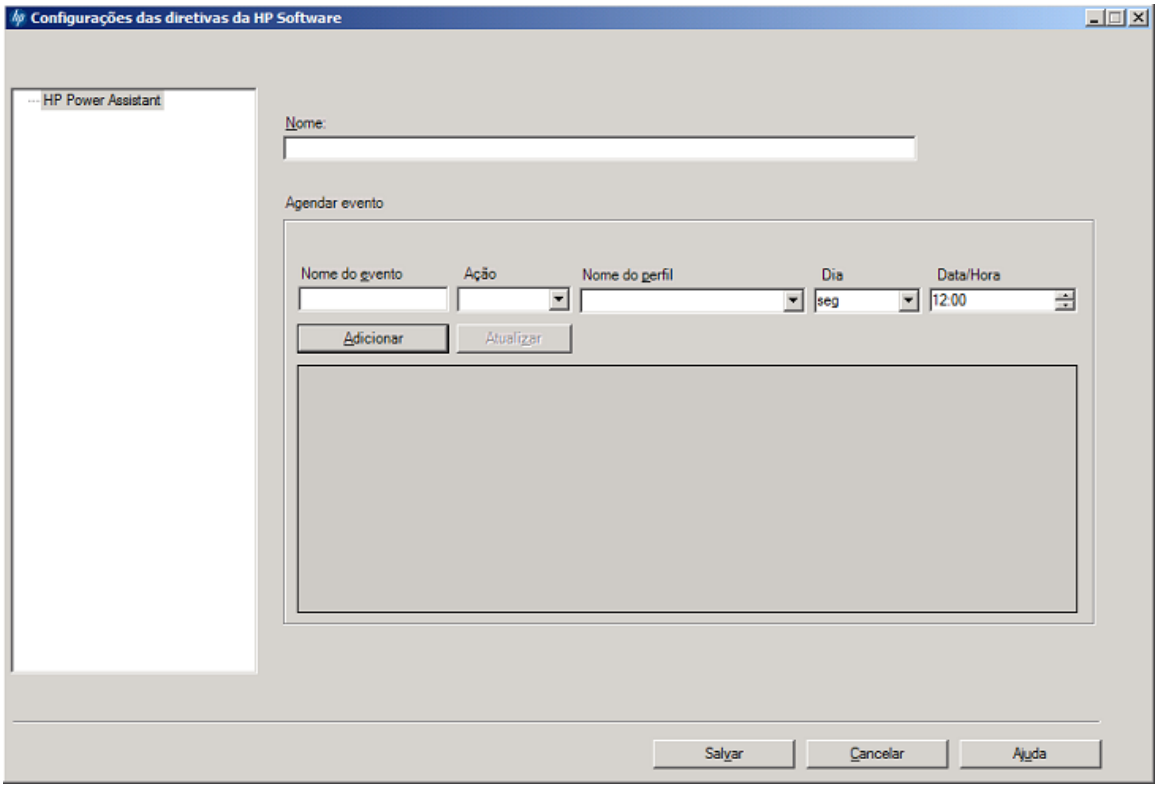
IMPORTANTE: Nova análise de inventário necessária para que as alterações de configurações do BIOS apareçam no Inventário
Qualquer alteração que você fizer na configuração do Assistente de energia da HP em um dispositivo gerenciado da HP usando a distribuição de uma tarefa de Diretiva de softwares da HP (Mudança de configurações) não será aplicado no inventário do dispositivo da HP até *após* a próxima Análise de inventário.

Para criar uma HP Software Diretiva definições (Power Assistant) pacote

1. No console, abra a ferramenta de **Configurações de segurança**.
2. Faça duplo-clique em Minhas **configurações de segurança** .



3. Clique com o botão direito do mouse **Diretivas de softwares de HP** , e, em seguida, clique em **Novo** . O Software HP Diretiva diálogo de configurações é exibida. É aqui é que você configura o Assistente de energia da HP que controla o comportamento de energia dos dispositivos gerenciados da HP.



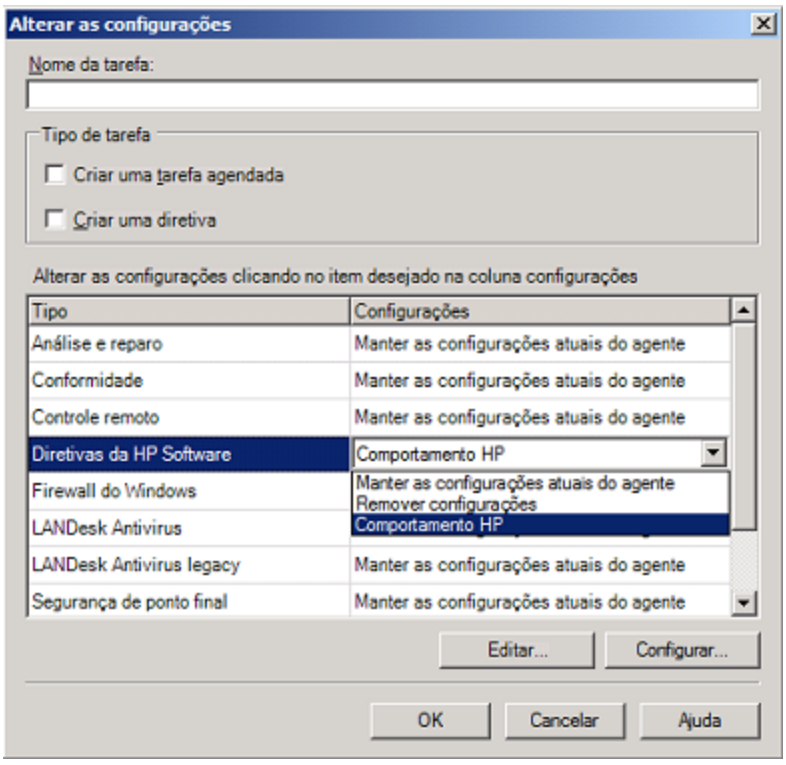
4. Digite um nome exclusivo para o pacote de configurações de diretivas de softwares da HP.

5. Insira um nome exclusivo para o evento específico que você está configurando. Um conjunto de configurações pode ser constituído de um ou mais eventos agendados para diferentes dias e/ou períodos de tempo.
6. No menu **Ação, selecione** o tipo de ação que você deseja este evento a realizar (Hibernate, sono, Sobre).
7. No menu **Nome do perfil,** selecione o perfil de energia predefinido da HP que pretende este evento para implementar (Econômico, Equilibrado, Otimizado, Alto desempenho).
8. Nos menus **Dia** e **Hora**, especifique quando quer aplicar o evento.
9. Clique em **Adicionar** para adicionar o evento na caxa de listas. Uma diretiva de software da HP e as configurações do Assistente de energia da HP associadas é definida pela combinação de um ou mais eventos.
10. Ao terminar a configuração das Diretivas de softwares da HP, clique em **Salvar** para armazenar as definições e fechar a caixa de diálogo. A nova diretiva aparece na lista, no frame da direita.

Agora, você pode implementar a diretiva, atribuindo-o a uma alteração de definições tarefa e, em seguida, usando a ferramenta Tarefas agendadas para especificar o tempo e alvo dispositivos HP.

Para criar um Alterar Definições tarefa com uma HP Software Diretiva

1. Na janela de ferramentas de configurações de segurança, clique no botão da barra de ferramentas **Criaruma tarefa** e em **Alterar configurações**.



2. Digite um nome exclusivo para a tarefa.
3. Especifique se pretende criar uma tarefa ou diretiva programada.

4. No menu suspenso das **Diretivas de softwares da HP**, selecione a diretiva que pretende implantar dispositivos de destino.
5. Clique em **OK** para salvar a tarefa e fechar a caixa de diálogo.

Tópicos relacionados

Agora você pode distribuir a configuração usando a ferramenta Tarefas agendadas. Para obter informações detalhadas sobre como usar a ferramenta Tarefas agendadas, veja:

"Agendamento de tarefas" na página 227

"Usar a janela Tarefas agendadas" na página 228

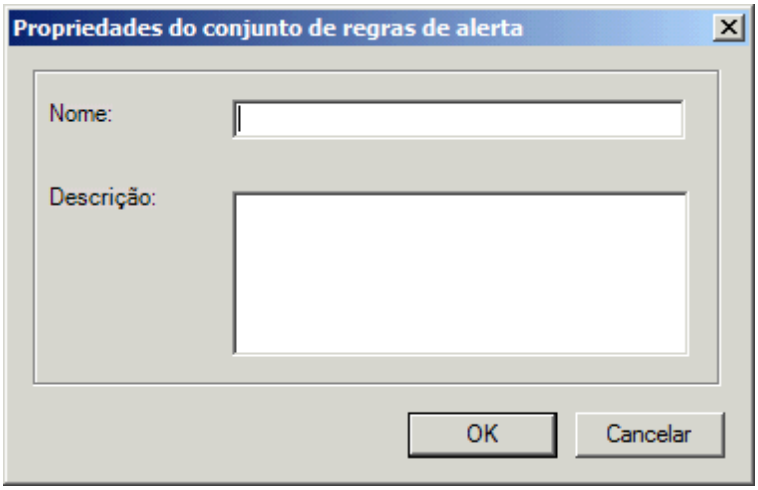
Configure alertas para dispositivos gerenciados HP

Você pode usar a ferramenta de Alertas da LANDesk para criar *conjuntos de regras* que monitora, mede e alerta caso ocorra um evento específico, condição seja satisfeita ou limite seja ultrapassado nos dispositivos da HP e nos periféricos para pontos-de-venda que você gerencia.

Conjuntos de regras personalizados disparam alertas para notificar você quando um dispositivo da HP ou algum atributo dos periféricos para pontos-de-venda de varejo (RPOS) — como voltagens, temperatura, uso da página da impressora etc. — exceder um limite especificado.

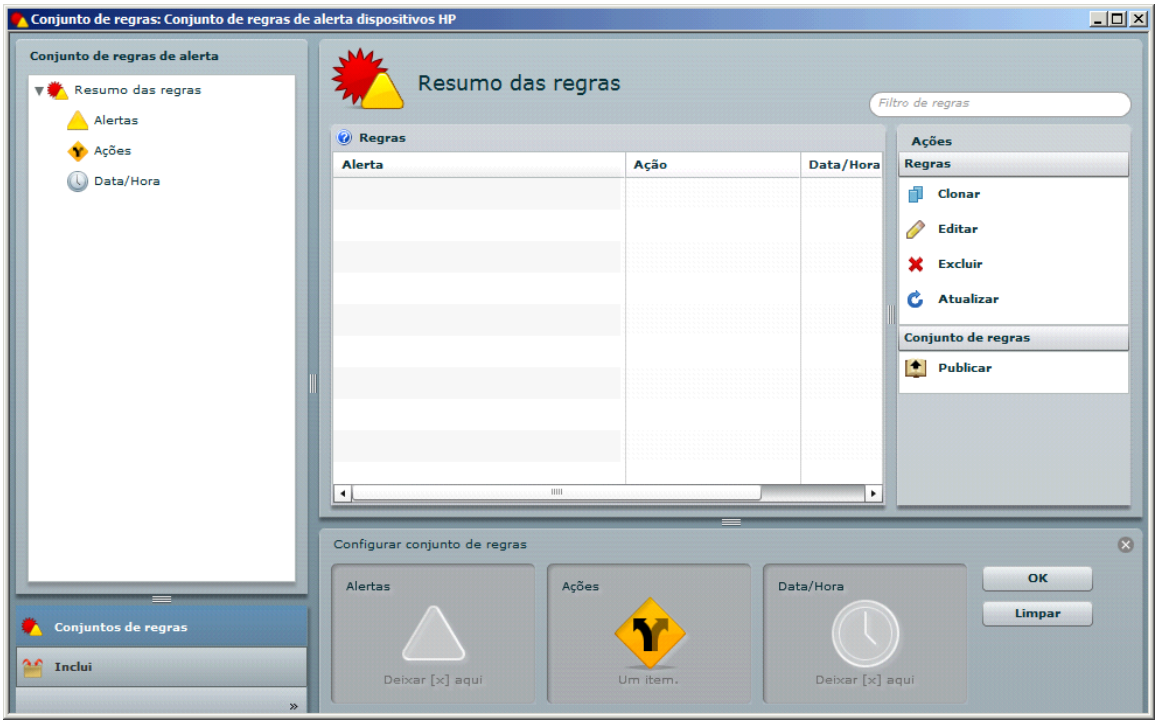
Para configurar alertas e conjuntos de regras de alerta

1. No console, clique em **Ferramentas > Configuração > Alertas**. A janela da ferramenta de alerta é exibida.
2. Clique no botão **Novo conjunto de regras de alerta** na barra de ferramentas.



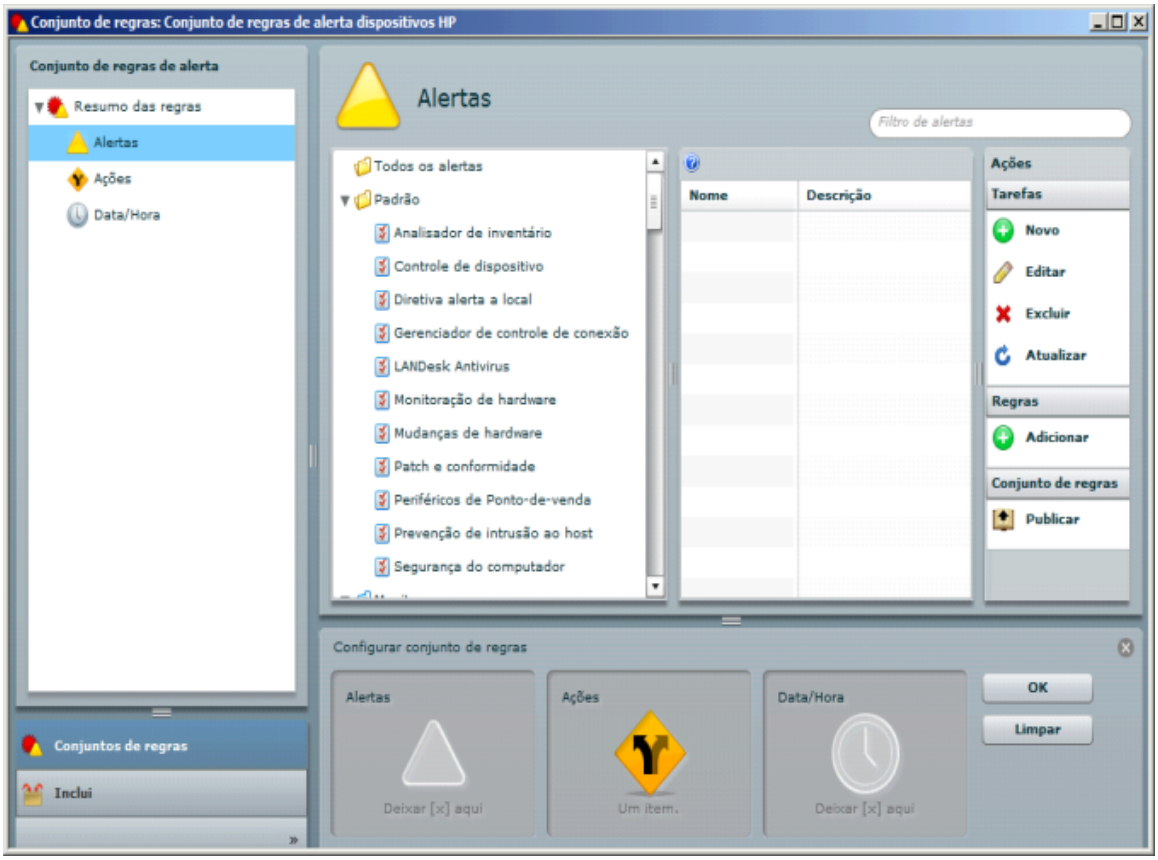
3. Insira um nome exclusivo e descrição para o novo conjunto de regras e clique em **OK**. O novo conjunto de regras é exibido na lista de Alertas.

4. Clique com o botão direito em conjunto de regras e em **Editar**.

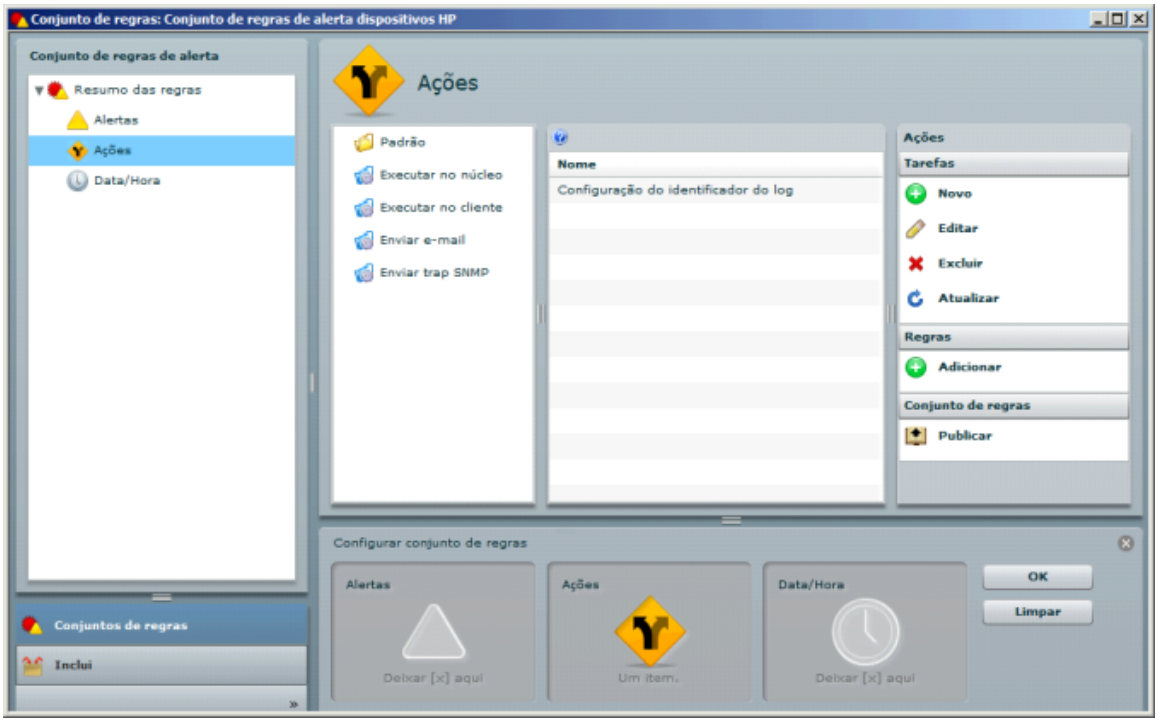


5. Na caixa de diálogo Resumo de regras, clique em **Alertas** para abrir a lista de alertas onde você pode selecionar o item sobre o qual quer ser alertado.

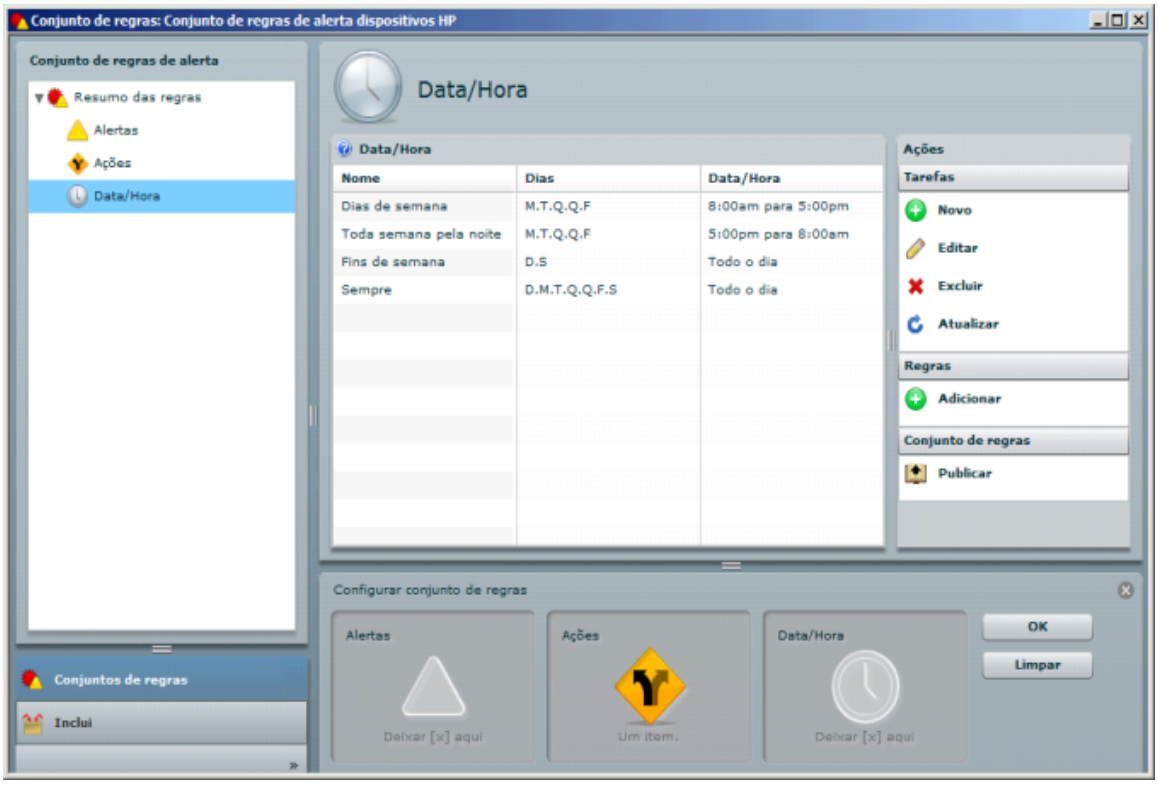
   O alerta de Periféricos de Ponto-de-venda está localizado sob o nó **Padrão**. Vários dispositivos da HP e periféricos RPOS e atributos estão localizados no nó **Monitor**. Navegue por esta lista para encontrar o componente ou recurso que você quer rastrear ou do qual você quer receber alertas.



6. Clique em **Ações** para abrir o painel de ações onde você pode especificar o comportamento do alerta.

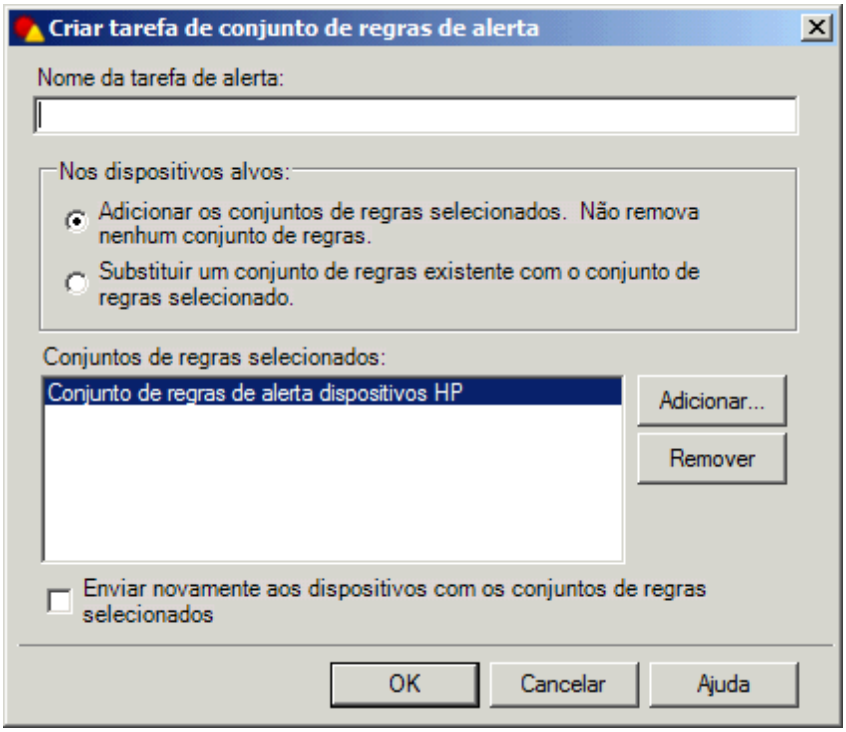


7. Clique em **Data/hora** para abrir o painel de opções de data/hora onde você pode especificar as configurações de data/hora para este alerta.



8. Clique em **Adicionar** para adicionar o alerta que você acabou de configurar para o conjunto de regras.
9. Ao terminar de compilar seu conjunto de regras, clique em **OK**.

10. Na janela da ferramenta de Alerta, clique com o botão direito no conjunto de regras que você quer distribuir nos dispositivos alvo da HP e clique em **Distribuir conjunto de regras**. (Ou, clique em **Criar uma tarefa** no botão da barra de ferramentas e em **Distribuir conjunto de regras**.)


Criar tarefa de conjunto de regras de alerta
Nome da tarefa de alerta:
Nos dispositivos alvos:
Adicionar os conjuntos de regras selecionados. Não remova nenhum conjunto de regras.
Substituir um conjunto de regras existente com o conjunto de regras selecionado.
Conjuntos de regras selecionados:
Conjunto de regras de alerta dispositivos HP
Adicionar...
Remover
Enviar novamente aos dispositivos com os conjuntos de regras selecionados
OK
Cancelar
Ajuda

11. Digite um nome para a tarefa de alerta, selecione se você quer adicionar o conjunto de regras selecionadas à qualquer um dos conjuntos de regras existentes no dispositivo alvo, clique em **Adicionar** ou **Remover** para personalizar os conjuntos de regras que você quer distribuir com esta tarefa e clique em **OK** para criar a tarefa e adicione-a à janela da ferramenta Tarefas agendadas.

Agora você pode usar a ferramenta Tarefas agendadas para distribuir a tarefa de alerta do conjunto de regras para os dispositivos alvo da HP que você desejar. Para obter informações detalhadas sobre o uso da ferramenta Tarefas agendadas, consulte "Agendamento de tarefas" na página 227 e "Usar a janela Tarefas agendadas" na página 228.

NOTA: Uso da ferramenta de Alerta da LANDesk
Para obter mais informações sobre o uso da ferramenta de Alerta da LANDesk, consulte a seção Alertas no *Guia do usuário* que começa com "Alertas" na página 790.

Configure relatórios para dispositivos gerenciados HP

A ferramenta Relatórios da LANDesk permite que você gere relatórios contendo informações críticas e em tempo hábil, usadas para identificar e resolver problemas, acompanhar dispositivos HP e periféricos de ponto-de-venda de varejo, registre e compartilhe essas informações importantes com as principais partes interessadas.

A ferramenta Relatórios permite que você execute relatórios em tempo real, crie tarefas agendadas de relatórios (PDF, XLS, DOC, CSV) e exporte relatórios.

Com a ferramenta Relatórios, você pode gerar:

- Relatórios padrão (Inventário)
- Relatórios específicos da HP (Fornecedor)
- Relatórios personalizados com base em consultas de banco de dados

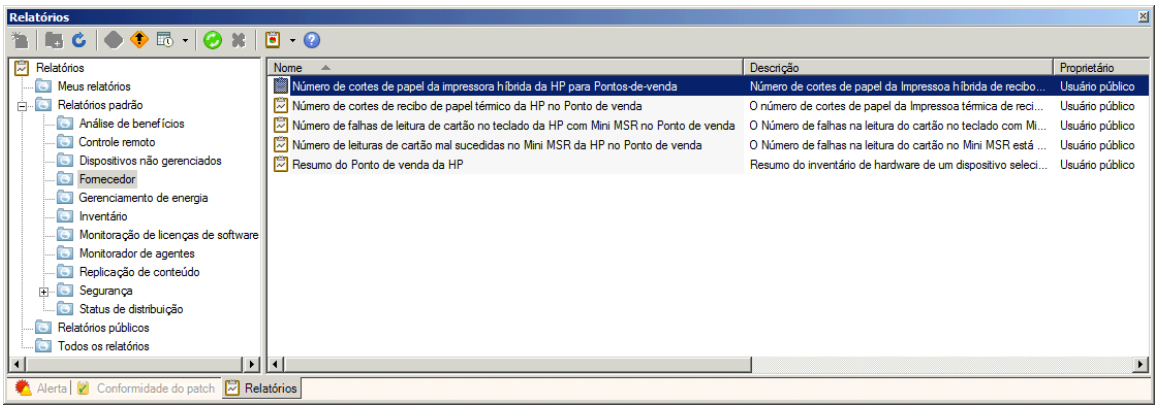
Relatórios da HP

A ferramenta integrada LANDesk Management Suite com Gerenciamento de hardwares da HP inclui diversos relatórios específicos da HP que são adicionados à ferramenta Relatórios durante a instalação do software da HP.

Relatórios HP:

- [NOVO] Verificador de bateria da HP (com dados de uma sistema de análise de diagnóstico do Verificador de baterias da HP, consulte "Use o Verificador de bateria da HP" na página 969)
- [NOVO] Informações do recurso Placa de rede móvel da HP (com dados a partir de uma análise de sistema do Gerenciador de conexões da HP, veja "Use o Gerenciador de conexões da HP" na página 970)
- Número de cortes de papel da impressora híbrida da HP para Pontos-de-venda
- Número de falhas de leitura de cartão no teclado da HP com Mini MSR no Ponto de venda
- Número de leituras de cartão mal sucedidas no Mini MSR da HP no Ponto de venda
- Resumo do Ponto de venda da HP
- Número de cortes de recibo de papel térmico da HP no Ponto de venda
- [NOVO] O Consumo de energia do Assistente de energia da HP (com dados de uma tarefa personalizada de configuração de diretivas de softwares da HP, consulte "Criar e distribuir configurações de diretivas de softwares da HP para dispositivos HP" na página 971)
- [NOVO] O Consumo de energia do Assistente de energia da HP por dia da semana (com dados de uma tarefa personalizada de configuração de diretivas de softwares da HP, consulte "Criar e distribuir configurações de diretivas de softwares da HP para dispositivos HP" na página 971)

Esses relatórios da HP estão localizados no grupo **Relatórios padrão > Fornecedor** na janela da ferramenta **Relatórios**.


Relatórios
Relatórios
Meus relatórios
Relatórios padrão
Análise de benefícios
Controle remoto
Dispositivos não gerenciados
Fornecedor
Gerenciamento de energia
Inventário
Monitoração de licenças de software
Monitorador de agentes
Replicação de conteúdo
Segurança
Status de distribuição
Relatórios públicos
Todos os relatórios
Nome
Descrição
Proprietário
Número de cortes de papel da impressora híbrida da HP para Pontos-de-venda
Número de cortes de papel da Impressoa híbrida de recibo...
Usuário público
Número de cortes de recibo de papel térmico da HP no Ponto de venda
O número de cortes de papel da Impressoa térmica de reci...
Usuário público
Número de falhas de leitura de cartão no teclado da HP com Mini MSR no Ponto de venda
O Número de falhas na leitura do cartão no teclado com Mi...
Usuário público
Número de leituras de cartão mal sucedidas no Mini MSR da HP no Ponto de venda
O Número de falhas na leitura do cartão no Mini MSR está ...
Usuário público
Resumo do Ponto de venda da HP
Resumo do inventário de hardware de um dispositivo seleci...
Usuário público
Alerta
Conformidade do patch
Relatórios

Gerando relatórios

Para gerar relatórios

1. No console, clique em **Ferramentas > Relatórios / Monitoramento > Relatórios**. A janela da ferramenta de Relatórios é exibida.
2. Para executar (e gerenciar) os relatórios de Inventário padrão, abra o grupo **Relatórios padrão** na visualização da árvore de Relatórios, clique no grupo **Inventário** e clique com o botão direito em um relatório específico na lista de relatórios do painel direito e clique em **Executar**. Especifique os parâmetros de relatório e, em seguida, clique em Exibir **Relatório**.
3. Para executar (e gerenciar) os relatórios específicos da HP, abra o grupo **Relatórios padrão** na visualização da árvore de Relatórios, clique no grupo **Fornecedor** e, com o botão direito, clique em um relatório específico da HP na lista de relatórios (veja a imagem acima) e clique em **Executar**. Especifique os parâmetros de relatório e, em seguida, clique em Exibir **Relatório**.
4. Para criar (e gerenciar) um relatório sob medida com base em consulta, clique com o botão direito em **Meus relatórios** e clique em **Novo relatório**. Digite um título exclusivo e descrição. Clique em **Carregar a partir da consulta do LDMS**, selecione a consulta ao banco de dados que você quer usar como critério para os relatórios sob medida e clique em **OK**. Especifique as outras opções de relatório desejadas e clique em **OK** para criar o relatório e salve-o no grupo Meus relatórios.

Para criar relatórios personalizados, antes você deve ter consultas de banco de dados baseadas em dados específicos de dispositivos da HP (e/ou dados de dispositivos RPOS). Você pode fazer isso com a ferramenta Consultas na Tela de rede do console.

NOTA: Uso da ferramenta Consultas da LANDesk
Para obter mais informações sobre o uso da ferramenta Consultas da LANDesk, consulte a seção Consultas no *Guia do usuário* que começa com "Gerenciador de diretórios/consultas" na página 183.

NOTA: Uso da ferramenta Relatórios da LANDesk
Para obter mais informações sobre o uso da ferramenta Relatórios da LANDesk, consulte a seção Relatórios no *Guia do usuário* que começa com "Relatórios" na página 197.

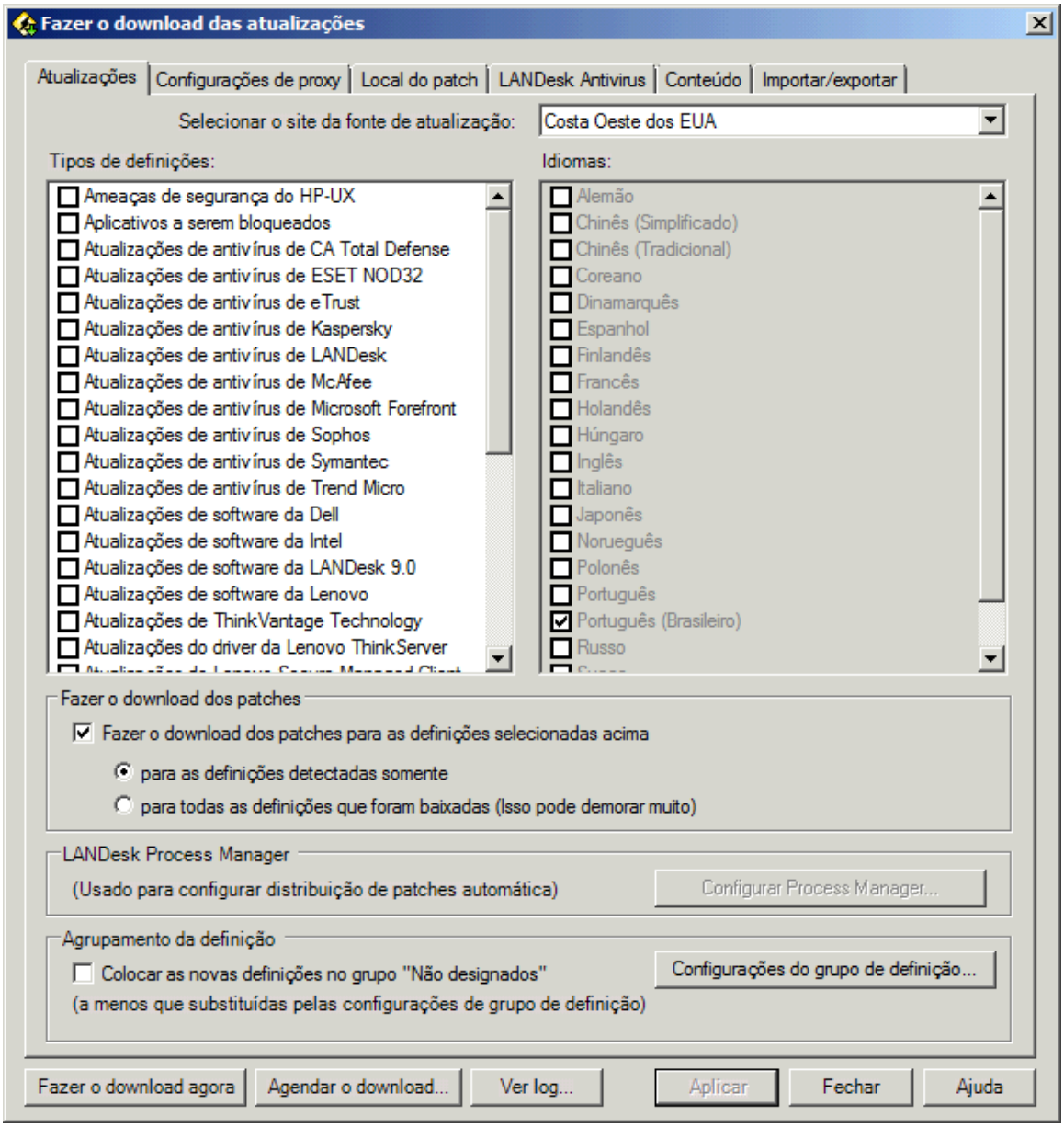
Faça o download e distribua as atualizações de softwares/drivers da HP

Você pode usar a ferramenta de Patch e conformidade do LANDesk Management Suite para fazer o download de pacotes de drivers e atualizações de conteúdo de BIOS da HP para mais recentes (atualizações "HP Softpaq") e distribuí-los para os dispositivos gerenciados da HP.

IMPORTANTE: Uma HP de específico conteúdo assinatura separada não é necessário, você
não precisa de uma subscrição especializada separada de conteúdo a fim de baixar o HP conteúdo específico com o LANDesk Patch e cumprimento Download ferramenta de atualizações. O conteúdo do Gerenciamento de hardwares e softwares da HP (atualizações HP Softpaq) é considerado o conteúdo padrão da LANDesk e está disponível para download com sua assinatura básica de softwares da LANDesk.

Para fazer o download de atualizações da HP

1. No console, clique em **Ferramentas > Segurança e Conformidade > Patch e conformidade**. A Janela da ferramenta de Patch e conformidade é exibida.
2. Clique o botão **Download de atualizações** na barra de ferramentas.



3. Na lista Tipos de definição, selecione **Atualizações da HP**.

4. Clique em **Fazer download agora** para iniciar o processo de download.

   OU

   Clique em **Agendar download** para criar uma tarefa agendada de download na ferramenta Tarefas agendadas.
5. Após concluir o download das atualizações de software da HP, você pode usar a ferramenta Patch e conformidade para exibir, filtrar e adicionar o conteúdo a uma tarefa de análise segurança/conformidade para distribuir as atualizações de software da HP para seus dispositivos gerenciados da HP.

NOTA: Uso da ferramenta de Patch e conformidade da LANDesk
Para obter mais informações sobre o uso da ferramenta de Patch e conformidade, consulte a seção Download de atualizações no *Guia do usuário* que começar com "Download das atualizações do conteúdo de segurança" na página 571.

Gerenciamento de dispositivos HP Thin Client a partir do console LANDesk

Depois de configurar os dispositivos Thin Client da HP com o agente padrão da LANDesk e de enviar para o banco de dados e inventário da LANDesk, você poderá usar várias ferramentas mais comuns da LANDesk para controlar e gerenciar os dispositivos.

Consulte a lista abaixo para Thin Client HP plataformas e quais as recursos e ferramentas do LANDesk são fornecidos para cada plataforma, além de uma breve descrição de cada ferramenta com um link para o seu principal tópico de visão geral da ajuda.

Compatível HP Thin Client plataformas de SO

LANDesk Management SuiteA versão9.5 oferece as recursos específicas listadas abaixo cada um dos seguintes suportados HP Thin Client plataformas.

Windows Embedded Standard 7 Enterprise (WES 7)

- LANDesk agent configuração (inventário, consultas) Standard
- Controle remoto
- Distribuição do software
- Gerenciamento de patches
- Gerenciamento do filtro de gravação

Windows Embedded Standard 09 Enterprise (WES 09)

- LANDesk agent configuração (inventário, consultas) Standard
- Controle remoto
- Distribuição do software
- Gerenciamento de patches
- Gerenciamento do filtro de gravação

HP ThinPro (Ubuntu)

- LANDesk agent configuração (inventário, consultas) Standard

Ajuda para configuração de parâmetros do BIOS

Este é o tópico de ajuda sensível a contexto do diálogo da configuração de parâmetros do BIOS no console LANDesk.

Use o diálogo para configurar parâmetros do BIOS que podem ser distribuídos entre seus dispositivos gerenciados HP.

IMPORTANTE: Nova análise de inventário exigida para que as alterações de parâmetros apareçam no inventário
Quaisquer alterações que você fizer no diálogo e distribuir para um dispositivo HP selecionado não se refletirão no inventário do dispositivo *até* a próximo Análise de inventário.

Esta caixa de diálogo contém as seguintes opções:

- **Seleção de parâmetros:**
  - **Aplicar somente as configurações modificadas nos clientes-alvo** Assegura que somente os parâmetros do BIOS que você alterou nesta configuração sejam aplicados aos dispositivos HP selecionados.
  - **Aplicar todas as configurações modificadas nos clientes-alvo** Assegura que *todos* os parâmetros do BIOS contidos nesta configuração sejam aplicados aos dispositivos HP selecionados.
- **Lista de recursos:**
  - **Recurso:** O nome do componente do BIOS HP.
  - **Configuração atual:** O valor especificado do componente do BIOS HP com base no último exame de inventário.
  - **Novo parâmetro:** O valor alterado que você deseja aplicar ao componente do BIOS HP.
- **Acesso do BIOS:**
  - **Senha atual do BIOS:** Permite acesso a dados do BIOS HP.
  - **Confirmar senha:** Exigido para acesso a dados do BIOS HP.
  - **Carregar parâmetros padrão do BIOS** Limpa os valores atuais dos componentes do BIOS HP e restaura os valores padrão do sistema.
- **Nome do pacote que será criado:**
  - **Nome do pacote de distribuição de software:** Identifica o pacote de software com um nome exclusivo.
- **OK:** Fecha o diálogo e salva o pacote de software na ferramenta LANDesk Software Distribution.
- **Cancelar:** fecha a caixa de diálogo sem salvar nenhuma alteração.

Tópicos relacionados

Parar obter instruções passo-a-passo sobre a configuração de parâmetros do BIOS HP que podem ser distribuídos para os dispositivos selecionados, consulte "Crie e distribua configurações de BIOS da HP para dispositivos HP" na página 963.

Ajuda para a configuração do TPM

Este é o tópico de ajuda sensível a contexto do diálogo da configuração de parâmetros do TPM no console LANDesk.

Use o diálogo para configurar parâmetros do TPM (Trusted Platform Module) security chip) que podem ser distribuídos entre seus dispositivos gerenciados HP.

IMPORTANTE: O Windows XP não é suportado
o HP chip TPM ferramenta de regulação não é suportada em dispositivos HP executando o sistema operacional Windows XP.

IMPORTANTE: Nova análise de inventário exigida para que as alterações de parâmetros apareçam no inventário
Quaisquer alterações que você fizer no diálogo e distribuir para um dispositivo HP selecionado não se refletirão no inventário do dispositivo *até* a próximo Análise de inventário.

Esta caixa de diálogo contém as seguintes opções:

- **Nome do pacote de distribuição de software:** Identifica o pacote de software com um nome exclusivo.
- **Opções de configuração do TPM** Determina os parâmetros do chip de segurança do TPM HP no dispositivo HP selecionado. (**NOTA:** Dependendo da opção que você selecionar, os campos de senha se alterarão conforme necessário para o acesso a dados do TM e a aplicação da nova configuração.)
- **Senha do BIOS:** Permite acesso a dados do BIOS HP.
- **Nova senha do TPM:** Permite acesso a dados do TPM HP.
- **Confirmar senha:** Exigido para acesso aos dados relevantes.
- **OK:** Fecha o diálogo e salva o pacote de software na ferramenta LANDesk Software Distribution.
- **Cancelar:** fecha a caixa de diálogo sem salvar nenhuma alteração.

Tópicos relacionados

Parar obter instruções passo-a-passo sobre a configuração de parâmetros do BIOS HP que podem ser distribuídos para os dispositivos selecionados, consulte "Crie e distribua configurações de chip TPM da HP para dispositivos HP" na página 966.

Ajuda para configurações de diretivas de softwares da HP

Este é o tópico de ajuda sensível a contexto do diálogo de Configurações de diretivas de softwares da HP na ferramenta de Configurações de segurança no console da LANDesk.

Use o diálogo para configurar os parâmetros do Assistente de energia da HP que podem ser distribuídos entre seus dispositivos gerenciados HP.

IMPORTANTE: Nova análise de inventário exigida para que as alterações de parâmetros apareçam no inventário
Quaisquer alterações que você fizer no diálogo e distribuir para um dispositivo HP selecionado não se refletirão no inventário do dispositivo *até* a próximo Análise de inventário.

Esta caixa de diálogo contém as seguintes opções:

- **Nome:** Identifica as configurações de diretivas com um nome exclusivo.
- **Agendar evento:**
  - **Nome do evento:** Identifica um evento específico da diretiva do Assistente de energia da HP. Você pode adicionar um ou mais eventos a fim de construir uma diretiva de energia personalizada.
  - **Ação:** Especifica a ação deste evento irá executar (hibernação, suspensão, ligar).
  - **Nome do perfil:** Especifica o perfil padrão de energia da HP (Econômico, Equilibrado, HP optimizado, Alto desempenho) para o evento que você está definindo.
  - **Dia:** Indica que dia(s) este evento será ativado em dispositivos alvo.
  - **Hora:** Indica o tempo de dia quando este evento será iniciado em dispositivos alvo.
  - **Adicionar:** Poupa o evento na caixa de lista. Você pode adicionar tantos eventos quantos quiser ao configurar uma diretiva de energia.
  - **Atualizar:** Guarda as alterações depois de clicar no ícone do lápis e fazer alterações em um evento.
- **Salvar:** Salva a diretiva e fecha a caixa de diálogo.
- **Cancelar:** fecha a caixa de diálogo sem salvar.

Tópicos relacionados

Parar obter instruções passo-a-passo das configurações de diretivas de softwares da HP que podem ser distribuídas para os dispositivos selecionados, consulte "Criar e distribuir configurações de diretivas de softwares da HP para dispositivos HP" na página 971.